Referaat IT-Auditing Opleiding

Groningen, juli 2012

Erasmus Universiteit Rotterdam

Postinitiële opleiding IT-Auditing and Advisory

Erasmus School of Accounting & Assurance (ESAA)

‘Trust audits en hun rol in het beoordelen van de robuustheid van ICT-ketens’

Dr. Ir. H.J.M. Bastiaansen – 351483

Begeleider: dhr. J. Pasmooij RE RO RA


trust

INHOUD


trust

Voorwoord

Voor u ligt mijn referaat ter afsluiting van mijn postdoctorale opleiding tot IT-auditor aan de Erasmus Universiteit te Rotterdam.

Het onderwerp dat ik voor dit referaat heb gekozen raakt aan mijn huidige interesse. Vanuit mijn werk bij TNO heb ik over de afgelopen jaren een persoonlijke ontwikkeling doorgemaakt in het type werkzaamheden en projecten waarbij ik betrokken ben. Naast onderzoeksprojecten ben ik steeds vaker betrokken geraakt bij projecten waarbij door organisaties aan TNO gevraagd is een oordeel of mening te geven over de kwaliteit van de inrichting van IT-infrastructuren en hun ondersteunende processen. Een taak uitstekend passend bij TNO als onafhankelijk onderzoeksinstituut en als organisatie met een groot spectrum aan technologische kennis.

Een aantal observaties heb ik bij het uitvoeren van deze werkzaamheden gedaan. Ten eerste, de inrichting van IT-infrastructuren en ondersteunende processen heeft (steeds meer) een organisatie-overschrijdend karakter, i.e. het terrein van ICT-ketens. Ten tweede, er is een gebrek aan raamwerken en normenkaders om ICT-ketens op een gedegen wijze te beoordelen. Tot slot, ik heb een 'onbevredigend buikgevoel' bij het uitvoeren van de beoordelingen van ICT-ketens. Dit laatste is gerelateerd aan de noodzaak dat ICT-dienstafnemers maar moeten vertrouwen dat hun toeleveranciers de dienstverlening met voldoende kwaliteit en conform afspraken nakomen, indien dergelijke afspraken überhaupt al (en met voldoende kwaliteit) zijn gemaakt. Kortom: naast de objectief en strikt meetbare en beoordeelbare criteria lijkt er voor het beoordelen van ICT-ketens ook ruimte te zijn voor en behoefte aan meer subjectieve criteria voor het vaststellen van vertrouwen tussen organisaties.

Het onderwerp van het beoordelen van ICT-ketens (en met name de rol van 'vertrouwen' tussen organisaties daarin) heeft hierbij mijn persoonlijke interesse gewekt. Gelukkigerwijs heeft dit onderwerp ook ruimte gekregen in de onderzoeksagenda van TNO. In een eerder stadium heb ik dan ook al aan dit onderwerp kunnen werken en de eerste gedachten hierover kunnen publiceren [BASTIAANSEN1]. Mijn interesse hierin werd verder bevestigd en gestimuleerd door een explorerend artikel over trust audits in een ICT-omgeving [ROSIELLE], waar ik door een collega van mij op gewezen werd.

Deze zaken combinerend was mijn persoonlijke keuze voor het onderwerp van mijn referaat ter afsluiting van de opleiding tot IT-auditor niet lastig: trust audits en hun rol in het beoordelen van de robuustheid van ICT-ketens. Hierbij besef ik wel dat dit onderwerp controversieel kan overkomen in de traditionele wereld van accounting en auditing. Het geven van zekerheid (assurance) op basis van objectieve vaststellingen is daar veelal het motto. Het instrument van trust-audit lijkt bij eerste aanblik daarmee op gespannen voet te staan. Mijn dank gaat derhalve uit naar de begeleiding vanuit de EUR voor het accepteren van dit onderwerp voor mijn referaat.

Tot slot wil ik wijzen op het Nederlandse onderzoeksproject TTISC (Towards Trustworthy ICT Service Chains) [TTISC]. Dit project werkt (o.a.) aan een overkoepelend raamwerk voor het beheersen en beoordelen van ICT-ketens. Daarbij wil ik mijn dank uiten voor de mogelijkheid om binnen dit TTISC- project (deels) mijn werkzaamheden aan dit referaat uit te voeren.

Groningen, juli 2012


trust

Management Samenvatting

In de maatschappij neemt het belang van ICT-ketens sterk toe. Bij ICT-ketens gaan ICT-diensten en infrastructuren over de grenzen van bedrijven en bedrijfsonderdelen heen. Niet alleen neemt het aantal ICT-ketens sterk toe, ook worden ze steeds complexer: ze ondersteunen meer functionaliteit en er zijn steeds meer partijen (ketenpartners) betrokken. Met dit toenemend belang van ICT-ketens neemt ook het belang van beheersing daarvan toe. Echter, bij ICT-ketens kan het een utopie blijken beheersing over de gehele keten uit te kunnen oefenen. In dat geval komt het aspect vertrouwen om de hoek kijken.

Dit referaat behandelt daarom de trust audit als instrument voor het vaststellen van de mate van vertrouwen in ketenpartners. We bedoelen daarbij met trust het vertrouwen dat organisaties in elkaar hebben om de in hun gestelde verwachting na te komen. Deze vorm van trust wordt ook wel aangeduid als inter-organisatorisch vertrouwen. Een trust audit geeft daarbij het instrument om de mate van trust vast te stellen. Deze definities sluiten goed aan bij de definities van ‘Organizational Trust’ zoals door het IIA (het Institute of Internal Auditors) gebezigd in hun research paper [IIAResearch].

Dit referaat beschrijft enerzijds de rollen die de trust audit kan vervullen als instrument voor ICT-ketenbeheersing en anderzijds de normatiek voor het uitvoeren van trust audits. De focus ligt daarbij op de beoordeling van de robuustheid van ICT-ketens.

Voor de beoordeling van de robuustheid van ICT-ketens worden in dit referaat een aantal rollen van trust audits beschreven die liggen op het terrein van de organisatorische en operationele beheersing van de kwaliteitsaspecten van de implementatie van een ICT-keten. Deze rollen zijn:

- het vaststellen van geschakelde ketens van vertrouwen tussen ketenpartners,
- het bijdragen aan een risico assessment van ICT-ketens,
- het bijdragen aan het kwantificeren van de mate van robuustheid van een ICT-keten.

In de uitwerking van de normatiek van de trust audit worden drie ‘aspecten’ onderscheiden voor het vertrouwen, elk met hun eigen normenkader:

- de ICT-dienst,
- de dienstaanbieder,
- het marktsegment.

Voor elk van deze drie aspecten van de trust audit wordt in dit referaat het normenkader uitgewerkt. Het wordt daarbij opgemerkt dat je formeel zou kunnen zeggen alleen al een goede normatiek voor de ICT-dienst voldoende zou moeten zijn. Eigenlijk hoef je namelijk ‘alleen maar’ betrouwbaarheid van het aangeleverde product te hebben. Echter, het uitgangspunt bij de trust audits is dat je dit niet (door kijken in de keuken van alle toeleveranciers) objectief kunt vaststellen. Dit rechtvaardigt het gebruik van de aanvullende aspecten

'dienstaanbieder' en 'marktsegment' in de normatiek als indirecte methode om betrouwbaarheid van het product op robuustheidseigenschappen vast te stellen.

Uit het onderzoek naar de trust audit voor dit referaat kunnen de volgende ***conclusies*** worden getrokken.

- Op een aantal terreinen voor het vaststellen van robuustheid van ICT-ketens kunnen trust audits een nuttige rol vervullen. Bovengenoemde rollen van de trust audit zijn als zodanig in dit referaat onderkend en uitgewerkt.

- Trust audits kennen ook hun beperkingen. Een trust audit doet geen strikte controle op de implementatie van de ICT-omgeving binnen individuele ketenpartners. De trust audit is dan ook niet een instrument waarmee 'positive assurance' kan worden verkregen met betrekking tot de robuustheid van ICT-ketens (vanuit ketenperspectief) of van individuele ketenpartners (vanuit partnerperspectief). De rol van de trust audit is inherent beperkt tot het kunnen bijdragen aan het afgeven van 'negative assurance'. Ook het 'omgekeerde' is niet het geval: vanuit de trust audit kun je ook niet stellen dat iets niet voldoet.

De ***aanbevelingen*** richten zich op twee aspecten:

- Het verder doorontwikkelen van de trust audits voor het beoordelen van robuustheid van ICT-ketens, bijvoorbeeld door

  (1) het opstellen en uitwerken van een toetsingskader,
  (2) het beproeven van de trust audit als methodiek in een aantal representatieve ICT-ketens, en
  (3) het uitwerken van de trust audits voor rollen in het beoordelen van robuustheid van ICT-ketens, aanvullend aan de rollen benoemd in dit referaat.

- Het uitbreiden van de scope van de trust audits buiten de scope van het beoordelen van robuustheid van ICT-ketens zoals beschreven in dit referaat. Deze scope uitbreiding kan bijvoorbeeld op:

  (1) het terrein van de strategische beheersing van ICT-ketens, en
  (2) het terrein van de ondersteunende processen voor de beheersing van ICT-ketens.

1. Inleiding

Dit hoofdstuk bevat het inleidende deel van het referaat. In de achtereenvolgende paragrafen van dit hoofdstuk komen aan de orde; het toenemend belang van ICT-ketens als aanleiding voor dit referaat (paragraaf 1.1), de beschouwing waarom beheersing van (inter-organisatorische) ICT-ketens anders is dan intra-organisatorisch ICT-beheersing (paragraaf 1.2), de onderliggende behoefte aan aanvullend instrumentarium voor het beoordelen van ICT-ketens in de vorm van trust audits (paragraaf 1.3), de doelstelling en onderzoeksvragen van het referaat (paragraaf 1.4), de werkwijze en aanpak (paragraaf 1.5), de scope-afbakening (paragraaf 1.6) en de leeswijzer voor dit referaat (paragraaf 1.7).

1.1 Aanleiding: Het toenemend belang van ICT-ketens

De huidige maatschappij kan niet functioneren zonder haar ICT-diensten en -infrastructuren. Het falen van onderdelen leidt tot (grootschalige) verstoringen van de processen en diensten die hiervan afhankelijk zijn. Zo kan bijvoorbeeld communicatiestoring bij een vervoersbedrijf leiden tot een ontregelde dienstregeling die veel reizigers treft, het falen van het elektronisch betalingsverkeer in het weekend voor kerst groot maatschappelijk ongenoegen tot gevolg hebben en falend Internet voor consumenten in het nieuwe werken resulteren in gemiste arbeidsproductiviteit.

Behalve dat het aantal ketens sterk toeneemt, worden ze ook steeds complexer. Enerzijds omdat de ketens meer functionaliteiten ondersteunen. Met een chipkaart wordt bijvoorbeeld een betaling verricht, maar daarvoor wordt ook gecheckt of de kaart niet gestolen is en wordt contact gelegd met de bank om het saldo te controleren. Anderzijds zijn steeds meer partijen betrokken in ICT-ketens. Het uitvoeren van alle functionaliteit van een chipkaart ligt bijvoorbeeld niet bij één partij maar bij meerdere (externe) partijen: de dienstaanbieder, een communicatie provider, financiële instelling, chipkaart register, enzovoorts.

Door de steeds toenemende vitaalheid van deze diensten is er steeds meer aandacht voor de beheersing van ICT-ketens en neemt ook de aandacht voor ICT-ketenaudits toe. Getuige hiervan zijn de Norea werkgroep voor ketenauditing [NOREA], onderzoeksinitiatieven bijvoorbeeld in de EU [ENISA] en Nederland [TTISC], [SEQUAL] en voorgaande publicaties in het Norea tijdschrift ‘de IT-auditor’ over ICT-ketenauditing [EDPAUDITOR1] – [EDPAUDITOR4].

1.2 Wat maakt de beheersing van (inter-organisatorische) ICT-ketens anders?

Voor de intra-organisatorische beheersing van ICT bestaat al een veelheid aan modellen en auditraamwerken. Voor inter-organisatorische beheersing van ICT (de ‘ICT-ketens’) is dit niet het geval. Wat maakt de beheersing van ICT-keten anders? Dit is een aantal aspecten.

In ICT-ketens is sterke governance niet een ‘gegeven’. Er is geen (strikte) ‘line of command’. De span of control voor individuele organisaties is beperkt. Vaak moeten beslissingen middels consensus worden genomen. Om

invloed te hebben is het voor individuele ketenpartners dan belangrijk om leiderschap te tonen tussen de andere ketenpartners.

Daarnaast zijn waarde, baten en doelstellingen niet eenduidig voor alle ketenpartners. Ketenpartners hebben een verschillende view op waarde en doelstellingen. Zij zullen andere voordelen van het werken in een keten nastreven en daarmee ook niet altijd opteren voor hetzelfde besluit in de keten. Er moet echter wel een gemeenschappelijk doel zijn, anders zou er geen sprake van een keten zijn. De kosten en baten zijn ook niet noodzakelijkerwijs evenredig verdeeld over alle ketenpartners. Daarom worden sommige baten niet automatisch behaald. Organisaties zullen niet investeren zonder zelf voldoende baten te kunnen realiseren. Het is belangrijk dit te realiseren wanneer er wordt beschouwd welke ketenpartners in een keten te betrekken.

Tot slot kunnen er communicatie- en cultuurverschillen zijn tussen ketenpartners. Zelfs binnen hetzelfde land kunnen verschillende sectoren specifieke terminologie hanteren. Organisatie-specifieke cultuur en communicatie kunnen effectief samenwerken in een keten beperken. Een gedeeld begrip en afstemming in de communicatie zijn van groot belang.

1.3 Behoefte aan aanvullend instrumentarium: de trust audit

Het is voor een partij niet altijd mogelijk ter controle in de keuken van hun toeleveranciers te kijken. Enerzijds is dat omdat deze toeleveranciers vanwege de bescherming van hun privacy en bedrijfsgeheim het niet wenselijk achten derden inzicht te geven in de (kwaliteit van de) inrichting van hun technische infrastructuur en/of operationele processen. Anderzijds is dit vanwege de praktische onuitvoerbaarheid (in tijd en budget), met name omdat er achter de toeleveranciers mogelijk weer een veelheid van andere toeleveranciers schuilgaat.

Voor het beheersen van robuustheid van ICT-ketens bestaat er al een aantal instrumenten:

- Voor het ***vastleggen*** van afspraken wordt gebruik gemaakt van Service Level Agreements (SLA's). In een Service Level Agreement (SLA) zal het bijvoorbeeld het beschikbaarheid niveau van de toeleverende dienst worden vastgelegd, in combinatie met straffen / penalties voor het geval hier door de toeleverancier niet aan wordt voldaan.

- Voor het ***vaststellen*** dat de toeleverancier daadwerkelijk aan gestelde robuustheidsafspraken voldoet, kan door de toeleverancier gebruik gemaakt worden van een verklaring hieromtrent door een onafhankelijke partij, bijvoorbeeld in de vorm van een TPM (SAS-70 of ISAE 3402 verklaring).

Voor ICT dienstcomponenten van toeleveranciers die een essentieel onderdeel uitvoeren van de ICT dienstverlening van een organisatie, zal de ketenverantwoordelijke zeer goed voor ogen moeten hebben of de derde partij zich aan gemaakte afspraken zal houden. Bij falen van de toeleverende ICT dienstcomponent zal de ketenverantwoordelijke er namelijk op worden aangesproken dat zijn dienst niet goed georganiseerd is. De vraag is daarbij of bovengenoemde instrumenten (SLA en TPM's) hem voor complexe ICT-ketens zekerheid zullen geven.

Zo komen we bij het lastige aspect van “vertrouwen in ICT-ketens”. Een ketenverantwoordelijk zal (behalve de SLA en TPM zelf) ook een beeld moeten vormen in hoeverre hij verwacht dat de derde partij eraan voldoet, hoe essentieel de ingekochte service is voor zijn dienst, en of hij eventueel maatregelen (b.v. redundantie of back-up) moet treffen voor het geval de derde partij de gemaakte afspraken niet nakomt. Het “blind” vertrouwen op de afspraken in de SLA is onvoldoende om in controle te zijn over de robuustheid van een ICT-keten.

Voor het vaststellen van de mate van beheersing over de robuustheid van een ICT-keten zijn aanvullende criteria nodig op het gebied van vertrouwen, met daaraan direct gekoppeld de vraag hoe betrouwbaar het hebben van vertrouwen is, bij voorkeur objectief en kwantitatief bepaald. Dit (objectief en kwantitatief) vaststellen van de mate waarin vertrouwen gesteld kan worden in toeleverende dienstcomponenten in ICT-ketens wordt omvat in het onderwerp Trust Audit. De uitkomst van een trust audit geeft als het ware een maat voor de “betrouwbaarheid van vertrouwen”.

Het wordt hierbij opgemerkt dat het instrument “trust-audit” controversieel kan overkomen en als “vloeken in de kerk” in de traditionele wereld van accounting en auditing. Daar heerst het beeld dat het geven van assurance gebaseerd dient te zijn op het objectief vaststellen van de mate van zekerheid, onder het adagium “Vertrouwen is goed, Controle is beter”[1]. Het instrument van trust-audit kan hiermee bij eerste aanblik op gespannen voet lijken te staan.

Daarnaast lijkt het instrument van een trust audit voor het vaststellen van de mate van “betrouwbaarheid van vertrouwen” op een interne tegenstrijdigheid. Vertrouwen gaat er toch juist over dat je niet alles controleert? Dit lijkt in tegenspraak met het doel van de audit, i.e. toch proberen een (op een objectieve wijze) een maat aan de betrouwbaarheid van dit vertrouwen te geven. Desalniettemin lijk het onderwerp van trust audits voldoende potentie als instrumentarium voor de auditor te hebben om een verdiepingsslag in dit referaat te rechtvaardigen, met daarbij speciale aandacht op de positionering van de trust audits.

1.4 Doelstelling en onderzoeksvragen

Gezien de aanleiding zoals geschetst in paragraaf 1.1 en de geïdentificeerde onderliggende behoefte aan aanvullend instrumentarium voor het beoordelen van de robuustheid van ICT-ketens in de vorm van trust audits (paragraaf 1.3), is de doelstelling van dit referaat:

1. het identificeren en beschrijven van potentiële rollen van het instrument van trust-audit in het objectief beoordelen van de robuustheid van ICT-ketens, en

2. het identificeren van normen waarmee (in een trust-audit) op objectieve en kwantitatieve wijze kan worden vastgesteld in welke mate vertrouwen gesteld kan worden in (de robuustheid van) toeleverende ketenpartners in ICT-ketens.

[1] De uitdrukking “Vertrouwen is goed, Controle is beter” wordt met regelmaat gebezigd in de wereld van auditing. De oorsprong van deze uitdrukking wordt echter toegeschreven aan een historisch persoon (Jozef Stalin) waar de wereld van auditing mijns inziens niet te veel associaties mee dient op te werpen, zie: http://nl.wikiquote.org/wiki/Jozef_Stalin.

Hierbij wordt het perspectief aangenomen vanuit een (ketenverantwoordelijke van een) organisatie die voor het leveren van zijn eigen ICT diensten een beroep doet op een veelheid van toeleverende ketenpartners (externe organisaties), die elk op zich ook weer hun eigen toeleveranciers kunnen hebben.

De onderzoeksvragen die in dit referaat worden behandeld ter beantwoording van bovengenoemde doelstelling zijn:

- Wat behelst een trust audit?
- Wat is de rol en belang van een trust audit in het objectief beoordelen van de robuustheid van ICT-ketens?
- Wat zijn normen waarmee (in een trust-audit) op objectieve en kwantitatieve wijze kan worden vastgesteld in welke mate vertrouwen gesteld kan worden in toeleverende dienstcomponenten in ICT-ketens?

1.5 Aanpak en werkwijze

Dit onderzoek is explorerend van aard. Het onderwerp van het kwantificeren van “betrouwbaarheid van vertrouwen” en het instrument van de trust-audit voor het geven van assurance in ICT-ketens staan nog in hun kinderschoenen. De literatuur over dit onderwerp is (zoals vooraf verwachting werd) nog beperkt.

Desalniettemin is het onderwerp van belang voor ICT-ketens, waarvoor (zoals in de inleiding aangegeven) het een utopie kan blijken te zijn om objectief vaststelbare zekerheid over de gehele keten van vele schakel en ketenpartners te geven. Als vanzelf zal het concept “vertrouwen” een grotere rol hierin gaan spelen.

Vanuit desktop onderzoek zal dit referaat antwoord geven op de vraag rondom meerwaarde, positionering en uitvoering van een trust audit als kwantitatief instrument om de robuustheid van ICT-ketens te beoordelen. Hierbij wordt voortgebouwd op een aantal eerdere, gerelateerde, onderzoeksinitiatieven bij TNO.

Vanuit literatuurstudie wordt gezocht naar een structuur voor en uitwerking van de normatiek voor trust audits. Op basis hiervan wordt een eerste, nog niet gevalideerde, versie van een normenkader voor trust audits opgesteld.

Indien als uitkomst van het onderzoek meerwaarde van deze trust audits zal worden vastgesteld, dan zullen daarbij aanbevelingen worden gedaan rondom de verdere praktische uitwerking hiervan.

1.6 Scope-afbakening

In de paragraaf 1.4 zijn al de doelstelling en onderzoeksvragen benoemd die in dit referaat zullen worden geadresseerd. De volgende aspecten vallen echter buiten de scope van het referaat:

- de uitwerking van toetsen voor het scoren van de normen voor een trust-audit,

- de validatie van het instrument van trust audit (met haar normen en toetsen) aan de hand van praktijk cases en/of statistische analyse van veelheid aan real-life casussen,
- de ontwikkeling van ondersteunende tooling.

1.7 Leeswijzer voor het referaat

Het vervolg van dit referaat heeft de opbouw zoals weergegeven in onderstaande tabel.

Hoofdstuk 2 **Trust audits voor het beoordelen van robuustheid van ICT-ketens: wat is het?**

In dit hoofdstuk wordt een verdere toelichting van het onderwerp van trust audits voor het beoordelen van robuustheid van ICT-ketens gegeven door de onderwerpen robuustheid en trust audit verder te verdiepen. Daarnaast bevat het hoofdstuk een eerste typering van het onderwerp trust audits binnen het raamwerk voor systeem-gerichte en productgerichte audit-aanpak van ICT-ketens.

Hoofdstuk 3 **Bronnenonderzoek**

In dit hoofdstuk wordt het bronnenonderzoek als basis voor de studie toegelicht Het hoofdstuk beschrijft de literatuurstudie, de inbreng van ISECOM / OSSTM en de afstemming met de Norea werkgroep voor ketenauditing (paragraaf 3.3).

Hoofdstuk 4 **De rol van trust audits voor het beoordelen van robuustheid van ICT-ketens**

Dit hoofdstuk benoemt en behandelt diverse rollen die trust audits kunnen vervullen voor het beoordelen van de robuustheid van ICT-ketens. De typologie van de ICT-ketens wordt beschouwd met speciale aandacht van de verschillende methoden van beheersing daarin. Achtereenvolgens komen daarna twee optieken aan de orde (de optiek van de ICT-keten en de optiek van een ketenpartner) van waaruit een rol voor een trust audit is voorzien bij het beoordelen van de robuustheid van een ICT-keten.

Hoofdstuk 5 **Normatiek voor trust audits**

Dit hoofdstuk werkt de normatiek voor trust audits uit. Het beschrijft het doel van de normatiek in trust audits. Het beschouwt inter-organisatorisch vertrouwen als basis om te komen tot een typologie voor inter-organisatorisch vertrouwen die de structuur geeft voor het inrichten van het normenkader voor trust audits. Tot slot geeft dit hoofdstuk een uitwerking van het normenkader voor trust audits.

Hoofdstuk 6 **Conclusies en aanbevelingen**

Dit hoofdstuk bevat de afsluitende conclusies en aanbevelingen van het onderzoek voor het referaat.

Aanvullend aan dit hoofddeel, bevat het referaat de volgende appendices:

***Appendix A*:** **Typologie van ICT-ketens**

Appendix B: **Bestaande normenkaders voor trust**

Appendix C: **Concept artikel '*(C^4-) model*'**


trust

2. Trust audits voor het beoordelen van robuustheid van ICT-ketens: wat is het?

De titel van dit referaat luidt: '*Trust audits en hun rol in het beoordelen van de robuustheid van ICT-ketens'*. In dit hoofdstuk wordt dit onderwerp verder toegelicht door de belangrijkste termen uit de titel verder uit te diepen. De scope van dit referaat wordt hiermee ook duidelijker afgebakend. De achtereenvolgende paragrafen uit dit hoofdstuk gaan daartoe verder in op de onderwerpen 'robuustheid van ICT-ketens' (paragraaf 2.1) en 'trust audit' (paragraaf 2.2), respectievelijk. Tot slot geeft paragraaf 2.3 een positionering van het onderwerp trust audits binnen het C^4-raamwerk voor de beheersing van ICT-ketens.

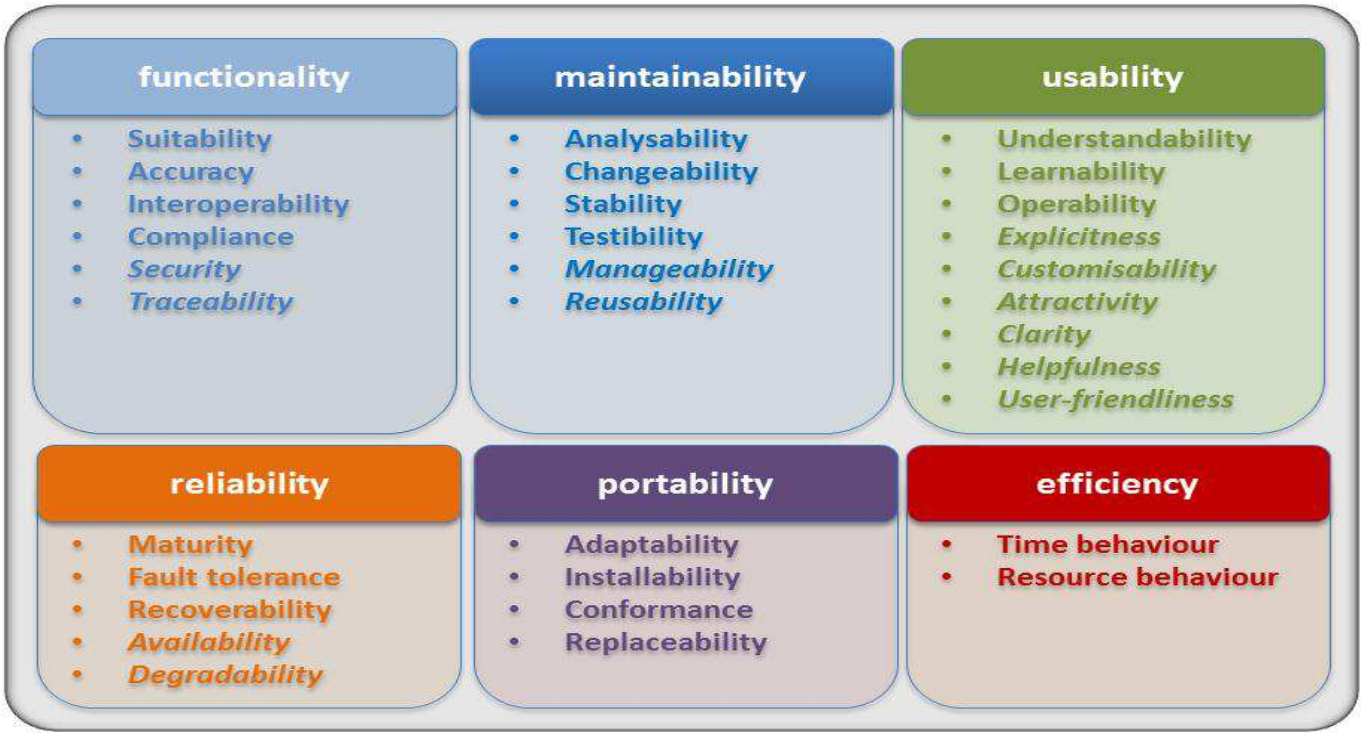
2.1 Wat bedoelen we met robuustheid van ICT-ketens?

Zoals beschreven in paragraaf 1.1 zijn we in het dagelijks leven in toenemende mate afhankelijk van de ICT-ketens. Het blijvend goed functioneren hiervan is daarmee van belang voor zowel de maatschappij als geheel als voor de individuele organisaties (of organisatieonderdelen) die afhankelijk zijn of onderdeel uitmaken van de ICT-ketens. De toename van het werken in ketens in combinatie met de groeiende complexiteit maakt de ICT-ketens ook in toenemende mate kwetsbaar.

In een omgeving waarin het belang van ICT-ketens steeds groter wordt, maar ook de kwetsbaarheid daarvan, is het de uitdaging voor organisaties (overheden en bedrijfsleven) om hun kritieke dienstverlening zeker te stellen. Indien de dienstverlening daarbij gebaseerd is op het intensief gebruik van ICT-technologie, dan betreden we het speelveld van robuuste ICT. Als definitie van robuustheid van een ICT-keten hanteren we daarbij:

> *"De robuustheid van een ICT-keten is de mate waarin aan de (kwalitatieve) verplichtingen van haar dienstverlening kan worden voldaan, onafhankelijk van de omstandigheden."*

In deze definitie gebruiken we de term '(kwalitatieve) verplichtingen'. Dit geeft aan dat robuustheid gericht is op de kwaliteit van de implementatie van ICT-ketens, en niet zozeer op andersoortige verplichtingen zoals financiële verplichtingen of compliance aan wet en regelgeving. Ook de term kwaliteit is daarbij een breed begrip. Voor de omschrijving van deze term verwijzen we naar de beschrijving en definitie van het breed palet aan kwaliteitseigenschappen voor software systemen zoals beschreven het Quint-model [QUINT], welke is afgeleid van de ISO 9126 norm voor kwaliteitskarakteristieken voor software systemen [ISO]. Figuur 1 geeft het overzicht van kwaliteitsaspecten waarop robuustheid van ICT-ketens van toepassing kan zijn. Het wordt daarbij opgemerkt dat de cursief weergegeven kwaliteitsaspecten de toevoeging in het Quint-model zijn ten opzichte van de ISO-norm.



Figuur 1: Kwaliteitsaspecten van software systemen volgens het Quint-model.

2.2 Wat bedoelen we met trust audits?

Trust is een breed begrip met veel verschillende betekenissen. Ook de term trust audit heeft diverse betekenissen. Nazoeken op Internet levert bijvoorbeeld al snel de volgende verschillende interpretaties van trust audits op:

- Trust audit in de wereld van de financiële accountancy. Hierbij wordt een beoordeling of assurance gegeven op (het beheer van) financiële fondsen.
- Trust audit voor de beveiliging van koppelingen tussen IT-systemen. Deze richt zich op de beveiligde koppeling en informatie-uitwisseling tussen computersystemen, vaak met focus op de kwaliteit en betrouwbaarheid van PKI-gebaseerde security implementaties.

Dit referaat behandelt echter een andere definitie van trust, te weten het vertrouwen dat organisaties in elkaar hebben om de in hun gestelde verwachting na te komen. Deze vorm van trust wordt ook wel aangeduid als inter-organisatorische trust of inter-organisatorisch vertrouwen. Ook deze termen zullen we in dit referaat gebruiken.

In dit referaat beschouwen we deze inter-organisatorische trust in de context van de robuustheid van de ICT-keten zoals beschreven in de vorige paragraaf.

Een veelheid aan definities van trust tussen organisaties bestaat. In [RATNASINGAM1], hoofdstuk 3, wordt een overzicht gegeven van de verschillende definities van trust zoals die in de literatuur zijn gegeven, specifiek voor inter-organisatorische trust. Deze definities zijn opgedeeld naar de verschillende terreinen van marketing, management, sociologie, psychologie en informatie systemen.

Als uitkomst van haar studie presenteert de auteur in [RATNASINGAM2] [RATNASINGAM3] ook een definitie van trust:

> *"The subjective probability with which organizational members collectively assess that a particular transaction will occur according to their confident expectations."*

De volgende elementen van deze definitie vergen aandacht:

- *'subjective'*

  Trust heeft per definitie iets subjectiefs in zich. Het heeft betrekking op aspecten die niet objectief vastgesteld zijn of vastgesteld kunnen worden, en die niet volledig voorspelbaar zijn. Trust en vertrouwen beginnen daarbij waar de kennis ophoudt [SYDOW1].

- *'probability'*

  Aan trust kun je een kwantificatie of score toekennen, die de mate van trust in iets weergeeft.

- *'according to their confident expectations'*

  Het object waarop trust van toepassing is dient te worden vormgegeven in lijn met de verwachtingen die daaraan worden gesteld. Dit deel van de definitie sluit goed aan bij onze definitie van robuustheid van een ICT-keten uit de vorige paragraaf.

Aansluitend bij deze bespiegelingen op de betekenis van trust, in combinatie met de definitie van robuustheid van een ICT-keten (uit de vorige paragraaf), hanteren we voor inter-organisatorische trust voor robuustheid van een ICT-keten in dit referaat als definitie:

> *"Inter-organisatorische trust voor robuustheid van een ICT-keten is de (subjectieve) mate waarin organisaties in de keten worden beoordeeld op het voldoen aan de (kwalitatieve) verplichtingen van haar dienstverlening, onafhankelijk van de omstandigheden."*

Deze definitie van trust zetten we op eenvoudige wijze door naar een definitie van trust audit. De trust audit wordt daarbij gedefinieerd als het instrument om de mate van trust zoals beschreven in bovenstaande definitie vast te stellen.

Tot slot dient het hier opgemerkt te worden dat deze definities goed aansluiten bij de definities zoals door het Institute of Internal Auditors (IIA) worden gebezigd in hun research paper [IIARESEARCH], onder de terminologie van 'Organizational Trust'.

2.3 Positionering van trust audit in het C^4 model voor ketenbeheersing

Bestaande modellen voor ICT-beheersing en auditing daarvan zijn veelal intra-organisatorisch gericht, en niet op ICT-ketens. Deze paragraaf beschrijft een model voor de beheersing van ICT-ketens. De (bestaande) auditraamwerken kunnen hierin worden gepositioneerd en worden aangepast om de specifieke ICT-keten aspecten te borgen. Het model helpt bij het identificeren van de hiaten in de beheersing van ICT-ketens en het geven van focus aan audits. Het model wordt aangeduid als het Chain Content & Context Control model (het C^4-model). Deze paragraaf geeft daarbij aan waar de trust audit in dit C^4-model gepositioneerd kan worden.

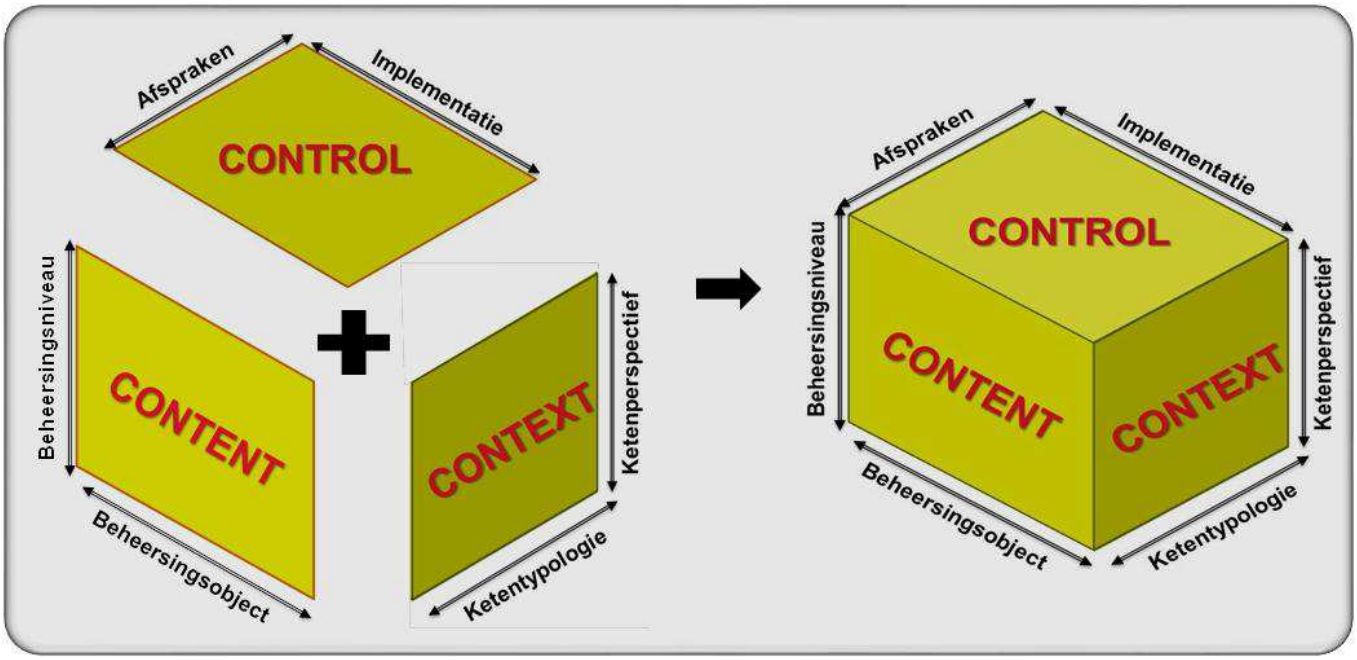
2.3.1 Het C^4 model voor ketenbeheersing met positionering van de trust audit

Voor het positioneren van de trust audits in de grotere context van de beheersing van ICT-ketens, maken we gebruik van het 'Chain Content, Context en Control model' (ofwel het 'C^4-model') voor de beheersing en controle van ICT-ketens, zoals beschreven in [BASTIAANSEN3] en opgenomen als Appendix C van dit referaat.

Het integraal C^4-model voor ICT-ketenbeheersing is door de auteur van dit referaat opgesteld uit behoefte aan een model om de uitdagingen aan ICT-ketenbeheersing vanuit diverse perspectieven op ICT-ketenbeheersing te positioneren, relateren en bespreekbaar / communiceerbaar te maken. Uit de recente onderzoeks- en audit-ervaringen bij TNO naar ICT-ketens bleek hieraan grote behoefte te zijn. In de literatuur bleek een dergelijk integraal model niet voorhanden te zijn. Dit nieuwe integrale C^4-model is daarbij opgesteld door zoveel mogelijk hergebruik te maken van bestaande modellen. Deze komen voornamelijk uit de methoden van intra-organisatorische ICT-beheersing, maar zijn in het C^4-model voor toepasbaar gemaakt voor ICT-ketenbeheersing.

Een basiseis aan een integraal model voor ICT-ketenbeheersing is dat het zowel de verschillende onderwerpen van ICT-ketenbeheersing (ofwel de 'content') benoemt, de verschillende perspectieven beschouwt van waaruit beheersing en beoordeling van ICT-ketens plaatsvindt (ofwel de 'context') als de methoden omvat waarop control kan worden uitgeoefend (ofwel de 'control').

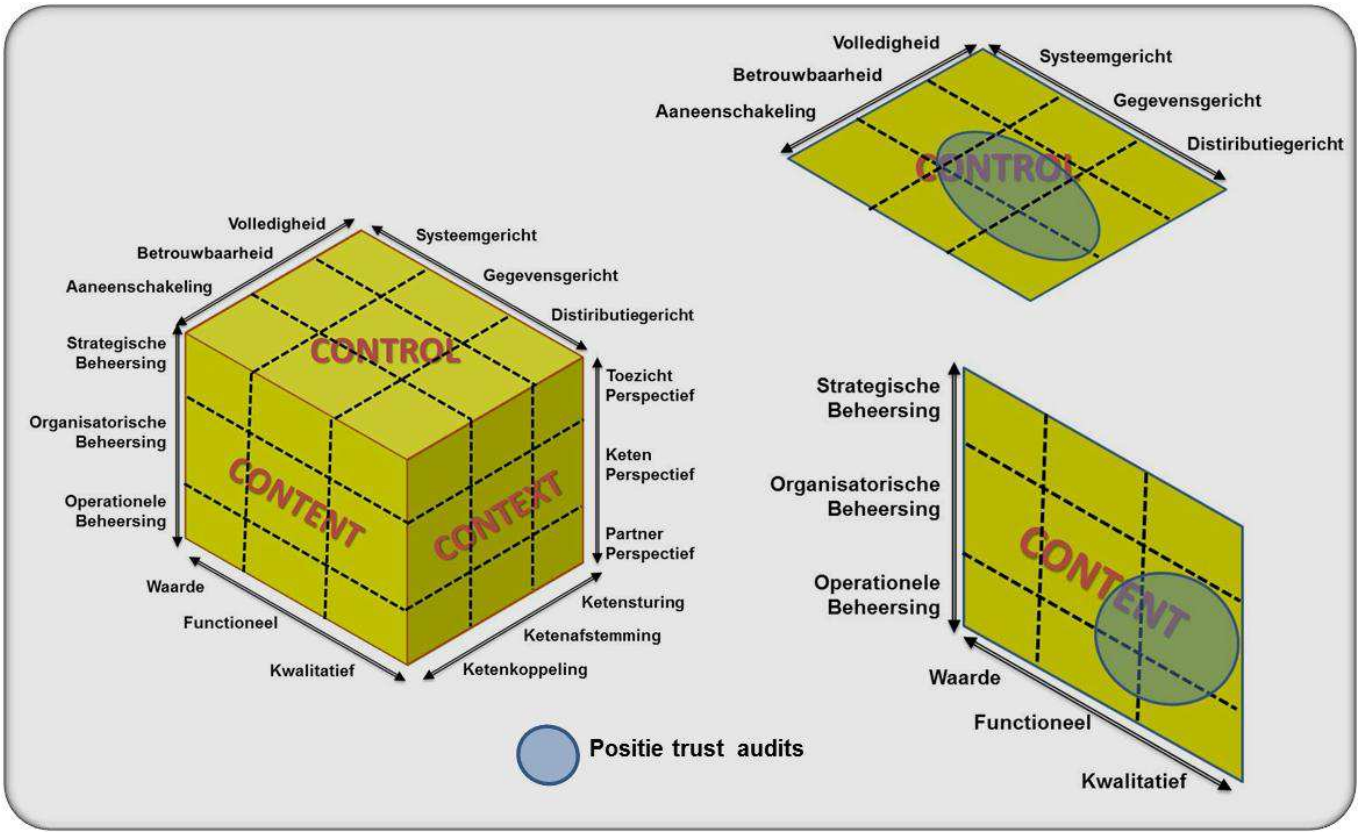
Het C^4-model omvat deze onderwerpen content, context en control. Het model splitst elke van de onderwerpen verder uit in twee assen, waardoor voor elk onderwerp een vlak ontstaat, i.e. het 'content-vlak', het 'context-vlak' en het 'control-vlak'. Het content-vlak wordt opgespannen door de as 'beheersingsniveau' en de as 'beheersingsobject', het context-vlak door de as 'ketentypologie' en de as 'ketenperspectief', en het control-vlak door de as 'afspraken' en de as 'implementatie'. Gecombineerd leiden de vlakken tot het integrale (kubusvormige) C^4-model voor ICT-ketenbeheersing, zoals weergegeven in Figuur 2.



Figuur 2: Het integraal C^4-model voor ICT-ketenbeheersing, opgebouwd uit een 'content'- 'context'- en 'control'-vlak.

Het wordt opgemerkt dat het combineren van de drie vlakken tot een kubus louter is bedoeld voor illustratieve doelstelling. Het combineren van drie 2-dimensionale vlakken in één enkele 3-dimensionale kubus zonder verlies aan informatie is uiteraard niet mogelijk. Bij het gebruik van de kubus (voor bijvoorbeeld het positioneren van ICT-audits) moet daarom worden teruggegrepen op de onafhankelijke vlakken, i.e. het content-vlak het context-vlak en het control-vlak.

In [BASTIAANSEN3] (Appendix C) worden het content-vlak, het context-vlak en het control-vlak met hun assen verder toegelicht, uitmondend in een detaillering van het integrale C^4-model, welke is weergegeven in Figuur 3. Deze figuur geeft daarbij ook positionering weer van de trust audit binnen het C^4-model voor de beheersing van ICT-ketens.



Figuur 3: Integraal C[4]-model voor ICT-ketenbeheersing met daarin de positie van de trust audit.

Zoals het rechterdeel van de figuur laat zien, is de trust audit voor het beoordelen van de robuustheid van een ICT-keten als volgt gepositioneerd:

- In het content-vlak binnen de kwalitatieve aspecten. De nadruk ligt daarbij in de organisatorische en operationele beheersing.
- In het control-vlak voornamelijk binnen de gegevensgericht en distributiegerichte aanpak. De nadruk ligt daarbij op de betrouwbaarheid en de aaneenschakeling van afspraken.
- In het context-vlak is er niet een specifieke perspectief of typologie waarop de trust audit van toepassing is. Derhalve is de positionering van de trust audit in het context-vlak niet in de figuur opgenomen.

In verband met de uitwerking van de diverse rollen die de trust audit kan vervullen (hoofdstuk 4), worden in de volgende subparagrafen de assen van het context-vlak verder toegelicht, i.e. de typologie van de ICT-keten en het perspectief op de ICT-keten.

2.3.2 Typologie van ICT-ketens

De typologie van de ICT-keten geeft de (types van) relaties weer die rollen in de ICT-keten ten opzichte van elkaar vervullen en de wijze waarop deze relatie wordt ingevuld.

Het startpunt van een typologie vormen de criteria op basis waarvan je verschillende types van ICT-ketens van elkaar gaat onderscheiden. Appendix A bevat een uitvoerige beschrijving van de typologie van ICT-ketens zoals we in dit referaat zullen hanteren. In deze subparagraaf beperken we ons tot een samenvatting op hoofdlijnen.

Voor het onderscheiden van ICT-ketens worden drie criteria gebruikt:

- de dynamiek van ICT-ketens,
- de invloed in ICT-ketens, en
- de topologie van ICT-ketens.

Binnen elk van deze criteria worden een aantal specifieke types onderscheiden, zie Appendix A. Deze drie criteria voor het onderscheiden van ICT-ketens zijn onderling onafhankelijk. Deze set van drie criteria vormt niet een ‘volledige’ set voor de typologie van ICT-ketens, maar is wel afdoende voor de scope van het referaat.

In het algemeen kunnen specifieke ICT-ketens niet worden gekarakteriseerd met een één-éénduidige keuze van opties (specifieke types) uit bovenstaande criteria. Specifieke ICT-ketens zullen (voor delen ervan) uit verschillende opties zijn opgebouwd: ze zijn hybride van aard.

De methoden waarop beheersing in een ICT-keten kan worden verkregen is in het bijzonder afhankelijk van de typologie van de ICT-keten). De mate van invloed in de ICT-keten is hier een belangrijk criterium in de typologie. De basis typen die daar worden onderscheiden zijn (zie Appendix A):

- *Ketenkoppeling*

  Bij ketenkoppeling werken ketenpartners met elkaar samen op basis afspraken over hun koppelvlak, zonder daarbij afstemming te hebben over de geleverde functionaliteit of de (kwaliteit van) de technische implementatie. Deze situatie treedt bijvoorbeeld op wanneer diensten op dynamische wijze middels service oriëntatie worden afgenomen.

- *Ketenafstemming*

  Bij ketenafstemming stemmen ketenpartners wel de functionaliteit en de kwaliteit op elkaar af. Op basis van consensus kunnen daarbij beslissingen worden genomen. Een voorbeeld hiervan is de situatie waarin ketenpartners op basis van gedeeld belang met elkaar de kwaliteit van hun technische implementatie bespreken, risico’s en zwakheden identificeren en eventueel tot (technische of procesmatige) compenserende maatregelen besluiten zoals bijvoorbeeld in [BASTIAANSEN2] beschreven voor het kwaliteitsaspect continuïteitsmanagement. Als speciale uitingsvormen hiervan

kunnen het afgeven van een Service Level Agreement (SLA) of een Third Party Mededeling (TPM) worden genoemd.

- *Ketensturing*

  Bij ketensturing is er sprake van een ketenpartner met voldoende overkoepelend gezag om eisen aan ketenpartners op te kunnen leggen over de wijze van invulling van hun ICT-voorzieningen. Dit zowel bijvoorbeeld doordat er een ketenpartner is met een dominante marktpositie of doordat er vanuit wet en regelgeving eisen worden opgelegd.

2.3.3 Perspectieven voor ICT-ketenbeheersing

In deze subparagraaf worden de toepassingen beschreven die worden voorzien voor de trust audit. De diversiteit aan toepassingen worden gecategoriseerd aan de hand van de optiek van waaruit de ICT-keten wordt beschouwd. De volgende optieken worden daarbij onderscheiden:

- *De optiek van de ICT-keten.*

  In deze optiek wordt de gehele ICT-keten van 'buitenaf' beschouwd ten einde te kunnen oordelen over de robuustheid van de keten en om risicogebieden in de ICT-keten te kunnen identificeren.

- *De optiek van een ketenpartner.*

  In deze optiek wordt de taak beschouwd van het op robuuste wijze verlenen van het eigen deel van ICT-dienstverlening vanuit een specifieke partij binnen de ICT-keten. In deze optiek wordt niet de gehele ICT-keten beschouwd maar slechts één enkele schakel hierin, met de nadruk op de betrouwbaarheid van de aan hem toeleverende ketenpartners (de 'naastliggende' schakels).

In hoofdstuk 4 worden potentiele rollen van de trust audit geïdentificeerd, waarbij vanuit beide optieken zal worden gekeken.

3. Bronnenonderzoek

In dit hoofdstuk wordt het bronnenonderzoek als basis voor de studie toegelicht. Zoals in het voorwoord van dit referaat aangegeven, werd mijn interesse voor trust audits als onderwerp van dit referaat gestimuleerd door een explorerend artikel over trust audits in een ICT-omgeving [ROSIELLE]. De resultaten uit dit artikel zijn voortgekomen uit een ISECOM project. Daarom zal paragraaf 3.1 eerst kort ingaan op ISECOM en haar werk aan de trust audits. Vervolgens beschrijft paragraaf 3.2 de literatuurstudie zoals uitgevoerd voor dit referaat. Paragraaf 3.3 gaat tot slot in op de afstemming met de Norea werkgroep voor ketenauditing .

3.1 ISECOM en haar werk aan trust audits

ISECOM (Institute for Security and Open Methodologies) is een open community en een non-profit organisatie gericht op het verbeteren van de wijze waarop beveiliging wordt geïmplementeerd en getest. Daarbij worden open methodieken nagestreefd.

In 2001 is ISECOM begonnen met het uitgeven van OSSTMM (de Open Source Security Testing Methodology Manual). Veel onderzoekers uit diverse gebieden dragen hieraan bij. De meest recente versie is OSSTMM v3 uit 2010. Momenteel wordt gewerkt aan OSSTM v4.

In OSSTM v3 heeft het onderwerp trust analyse een prominente plaats gekregen [ISECOM]. Daarmee is ook het onderwerp “trust audit’ op de kaart gebracht. Het hoofdstuk “Trust Analysis” uit OSSTM v3 [ISECOM] is tevens bewerkt tot een artikel in het tijdschrift Informatiebeveiliging [ROSIELLE]. Appendix B (Tabel 8) geeft het overzicht van de aspecten die vertrouwen tussen bedrijven bepalen, afkomstig uit dit artikel. Inmiddels verzorgt ISECOM ook opleidingen en certificering tot trust auditor.

3.2 Literatuurstudie naar trust audits.

In de volgende subparagrafen worden achtereenvolgens de aanpak van de literatuurstudie en de resultaten van de literatuurstudie (op hoog niveau) weergegeven.

3.2.1 Aanpak van de literatuurstudie

Deze subparagraaf beschrijft de aanpak die is gevolgd voor het uitvoeren van de literatuurstudie.

Uitgaande van een eerste (high-level) artikel over trust-audits is een eerste Internet zoek actie gedaan naar literatuur op het onderwerp trust audits in ICT-ketens. Het primaire doel hiervan was om de juiste terminologie te achterhalen zoals in (wetenschappelijke) literatuur wordt gebruikt voor het aanduiden van trust (en trust audits) zoals bedoeld in dit referaat. Als uitkomst van deze activiteit bleek dat in de wetenschappelijke literatuur

de term trust zoals bedoeld in dit referaat met name wordt aangeduid onder de termen ‘organisational trust’ of ‘inter-organisational trust’.

Op basis van deze terminologie voor trust in wetenschappelijke literatuur in combinatie met diverse termen voor ICT in ketens, is een aantal zoektermen gedefinieerd. Deze zoektermen zijn gebruikt in een literatuurzoektocht in de on-line wetenschappelijke bibliotheek van de EUR.

Aanvullend is voor de meest relevante publicaties gekeken naar welke (wetenschappelijke) publicaties zij verwezen. Ook deze zijn vervolgens opgezocht en (waar relevant) in het onderzoek meegenomen en opgenomen in de lijst van referenties.

3.2.2 Resultaten van de literatuurstudie

Na het doornemen van deze publicaties zijn de voornaamste inhoudelijke resultaten van de literatuurstudie.

- Er is veel onderzoek gedaan naar trust en haar eigenschappen, zowel met betrekking tot interpersoonlijke trust als inter-organisatorische trust.
- Wetenschappelijke literatuur op het gebied van inter-organisatorische trust ten behoeve van ICT-ketens is aanwezig, maar beperkt.
- Toepassing van inter-organisatorische trust op het terrein van auditing in ICT-ketens is minimaal.

Op basis van deze observaties trekken we de conclusie dat het onderwerp van dit referaat nog slechts minimaal in de wetenschappelijke literatuur beschreven is. Dit geeft daarbij tevens de rechtvaardiging voor het studieobject in dit referaat en opent de weg naar (wetenschappelijke) publicatie van de resultaten van de studie zoals beschreven in dit referaat.

3.3 De Norea werkgroep voor ketenauditing

Op het gebied van ketenauditing is een werkgroep van Norea actief [NOREA]. In het tijdschrift de EDP-auditor is een aantal artikelen gepubliceerd waaraan door de leden van de werkgroep is bijgedragen [EDPAUDITOR1] - [EDPAUDITOR4]. De nadruk bij de activiteiten van de werkgroep en de publicaties in het tijdschrift de EDP-auditor ligt daarbij op de rol en wijze van samenwerking van de auditdiensten van bij overheidsketens betrokken departementen.

De raakvlakken van dit werk met het onderwerp van trust audits zoals wordt uitgewerkt in dit referaat is echter minimaal. Daarom zal er in dit referaat niet verder op worden doorgebouwd.

4. De rol van trust audits voor het beoordelen van robuustheid van ICT-ketens

Dit hoofdstuk benoemt en behandelt diverse rollen die trust audits kunnen vervullen voor het beoordelen van de robuustheid van ICT-ketens. Paragraaf 4.1 beschouwt daarvoor als eerste de positionering van trust audits in de auditmethodiek voor ICT-ketens. Dit leidt voor het vervolg van dit hoofdstuk tot de verschillende rollen die voor een trust audit worden voorzien bij het beoordelen van de robuustheid van een ICT-keten (paragraaf 4.2): de rol van de trust audit voor het beoordelen van geschakelde ketens van vertrouwen tussen ketenpartners (paragraaf 4.3), voor het uitvoeren van risico assessments (paragraaf 4.4) en voor het kwantificeren van de mate van beheersing over de robuustheid in ICT-ketens (paragraaf 4.5).

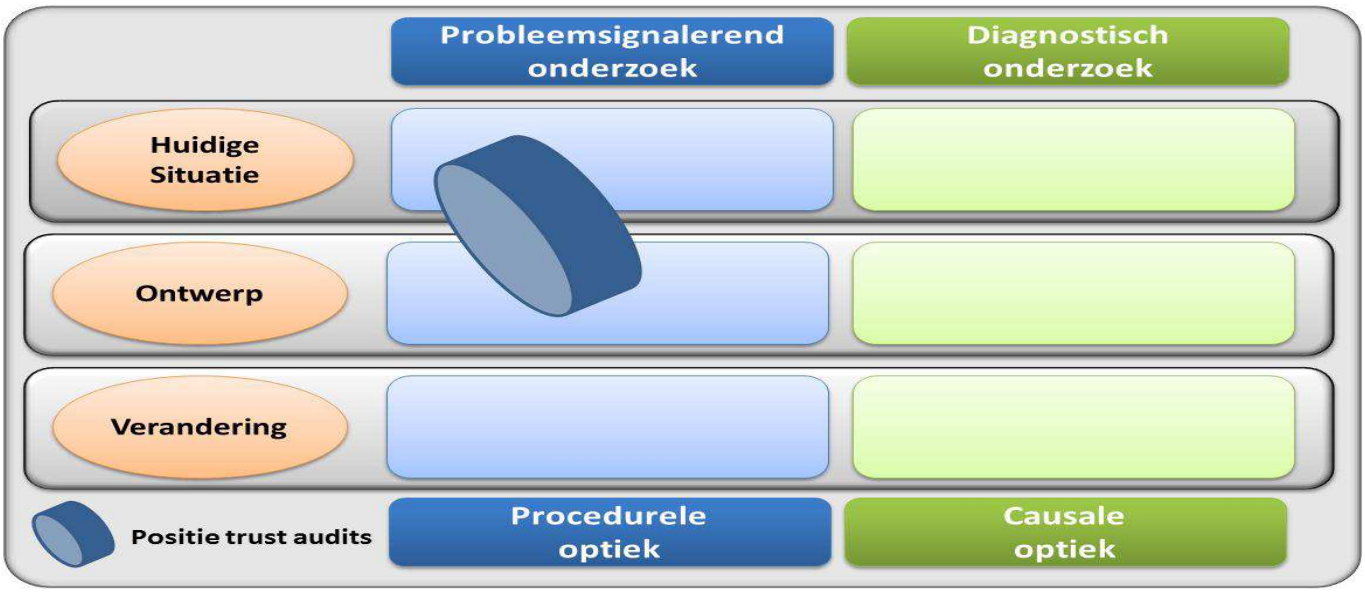
4.1 Positie van trust audit in de auditmethodiek voor ICT-ketens

We beginnen deze paragraaf met het herhalen van de definitie van robuustheid van ICT-ketens, zoals toegelicht in hoofdstuk 2:

> *"De robuustheid van een ICT-keten is de mate waarin aan de verplichtingen van haar dienstverlening kan worden voldaan, onafhankelijk van de omstandigheden."*

Een trust audit is gericht op het vaststellen van de mate van vertrouwen in ketenpartners. In dit referaat richten we ons daarbij op de vraag hoe een trust audit daarbij kan bijdragen aan het vaststellen van de mate van de robuustheid van een ICT-keten volgens bovenstaande definitie.

Een trust audit doet geen strikte controle op de implementatie van de ICT-omgeving binnen individuele ketenpartners. De positie van de trust audit in de auditmethodiek voor ICT-ketens m.b.t. audittypen en interventiecyclus is daarom zoals weergegeven in Figuur 4.



Figuur 4: Positionering trust audit in audit methodiek: audittypen en interventiecyclus.

Zoals de figuur aangeeft kan het volgende worden opgemerkt m.b.t. de positionering van de trust audit binnen de auditmethodiek:

- de positie van de trust audit is binnen de probleemsignalerende audits;
- in de interventiecyclus is de positie van de trust audit gericht op de huidige situatie en/of het ontwerp.

Omdat een trust audit geen strikte controle op de implementatie van de ICT-omgeving binnen individuele ketenpartners, is het niet geschikt als een instrument waarmee 'positive assurance' kan worden verkregen met betrekking tot de robuustheid van ICT-ketens (vanuit ketenperspectief) of van individuele ketenpartners (vanuit partnerperspectief). Ook het 'omgekeerde' is niet het geval: vanuit de trust audit kun je ook niet zeggen dat iets niet voldoet. De rol van de trust audit is hierdoor inherent beperkt tot het kunnen bijdragen aan het afgeven van 'negative assurance'.

Naast bovenstaande positionering van de trust audits binnen de auditmethodiek (met focus op audittypen en interventiecyclus), is het nodig om te beschouwen wat de rol van trust audits kan zijn in het uitvoeren van controles. Hiervoor wordt aangesloten op de methodiek van een 'top-down beoordeling' voor het uitvoeren van een controle, zoals bijvoorbeeld beschreven in [SCHILDER], paragraaf 2.3. In verkorte vorm is deze controle-aanpak weergegeven in Figuur 5, met daarin ook de rol van de trust audit aangegeven.

Figuur 5: Positionering van de trust audit in de top-down controle-aanpak.

Zoals de figuur laat zien ligt de rol van de trust audit in de controle-aanpak voornamelijk in het bijdragen aan de risico-assessment, aan het begin van de activiteiten van de top-down controle-aanpak. De rol van de trust audit in de controle op de interne beheersing is beperkt. De reden hiervoor is ook nu weer gelegen in het feit dat een trust audit geen strikte controle doet op de implementatie van de ICT-omgeving binnen individuele ketenpartners.

4.2 De rol van trust audits voor het beoordelen van robuustheid van ICT-ketens

Op basis van de beschouwingen in de vorige paragraaf worden de volgende rollen voorzien voor de trust audit bij het uitvoeren van een beoordeling op de robuustheid van een ICT-keten.

- Het vaststellen van geschakelde ketens van vertrouwen tussen ketenpartners.

Voor een partij in de ICT-keten is het optimaal als hij kan vertrouwen op de kwaliteitsafspraken met zijn directe ketenpartners en dat deze het benodigde niveau van compenserende maatregelen hebben genomen tegen eventuele onbetrouwbaarheid van hun achterliggende toeleveranciers. Deze 'achterliggende' toeleveranciers kunnen dan verder buiten de scope van de ketenpartner worden gehouden. Er ontstaat dan een geschakelde keten van vertrouwen. Geschakeld vertrouwen kan op diversie manieren worden gerealiseerd.

- Het bijdragen aan een risico assessment van de ICT-keten.

  Een risico-assessment op de robuustheid van de ICT-keten kan bijdragen geven aan de scoping van de meest relevante te onderzoeken aspecten en de benodigde effort voor het uitvoeren van het onderzoek aanzienlijk beperken. De trust audit kan hierbij als onderdeel van de risico-assessment een rol vervullen in het identificeren van risicogebieden en/of risico onderwerpen in de ICT-keten.

- Het bijdragen aan het kwantificeren van de mate van robuustheid van een ICT-keten.

  Voor het beoordelen van robuustheid van ICT-ketens geeft de mogelijkheid van het kwantificeren hiervan aanvullende informatie over de mate van robuustheid. Hierbij kan een trust audit bijdragen aan verschillende aspecten waarop de robuustheid van ICT-ketens kwantitatief kan worden beoordeeld.

Met de uitkomst van de bovenstaande rollen van de trust audits kunnen de stakeholders in de ICT-keten (indien benodigd geacht) vervolgstappen maken in het verbeteren van de robuustheid van ICT-ketens. Dit kan eventueel worden vormgegeven door de relaties tussen ketenpartners te veranderen (de ICT-keten als het ware anders in te richten, bijvoorbeeld als onderdeel van het procuratieproces), of aanvullende controle en compenserende maatregelen in te voeren. Deze aspecten van het aanpassen en herinrichten van de ICT-keten zijn een logische vervolgstap op de trust audits, maar vallen buiten de scope van dit referaat.

In de volgende paragrafen van dit hoofdstuk worden bovengenoemde rollen voor een trust audit bij het beoordelen van de robuustheid van een ICT-keten verder uitgediept.

4.3 Geschakelde keten van vertrouwen

Vanuit de optiek van een ketenpartner is er sprake van beheersing van de robuustheid van een ICT-keten als er een situatie is waarbij deze erop kan vertrouwen dat zijn directe ketenpartner (ofwel zijn toeleveranciers, inclusief alle achterliggende, voor hem "verborgen" ketenpartners / toeleveranciers) hem het gewenste en afgesproken niveau van dienstverlening leveren, zodat hij zijn eigen verplichtingen kan nakomen.

Een belangrijk aspect hierin is dat een ketenpartner zijn 'naaste' toeleveranciers kan vertrouwen. Als zijn 'naaste' toeleveranciers namelijk betrouwbaar zijn, dan kan de ketenpartner er vertrouwen in hebben dat deze het benodigde niveau van compenserende maatregelen heeft genomen tegen eventuele onbetrouwbaarheid van hun achterliggende toeleveranciers. Hoe verder weg toeleveranciers in de keten vanuit de optiek van de ketenpartner zijn, hoe minder belangrijk deze zijn voor de ketenpartner omdat deze mag verwachten dat een tussenliggende toeleverancier de vereiste compenserende maatregelen heeft genomen. Op deze wijze ontstaat

een ‘geschakelde keten van vertrouwen’, waarbij ketenpartners kunnen bouwen op het vertrouwen dat ze hebben in hun naaste toeleveranciers.

Drie methodes om een geschakelde keten van vertrouwen te realiseren kunnen worden onderscheiden. Deze drie methodes hebben een relatie met de typologie van de ICT-keten (zoals kort beschreven in paragraaf 2.3.2 en uitgediept in Appendix A), met name op het criterium van de mate van invloed in de ICT-keten. De drie methodes die worden onderscheiden zijn:

- *Op basis van controle of certificatie*

  Hiervan is sprake indien de betrouwbaarheid van de ketenpartner gecontroleerd is en middels certificatie bevestigd. Een eerste vorm hiervan kan zijn dat deze controle is uitgevoerd door een onafhankelijke derde partij en is vastgelegd in bijvoorbeeld de vorm van een Third Party Mededeling (TPM). De vraag is daarbij echter wel of de TPM het juiste object van de robuustheid afdekt, inclusief de achterliggende partijen in de ICT-keten.

  Een andere vorm van het verkrijgen van geschakeld vertrouwen is het afgeven van certificatie hiervoor door een hiervoor bevoegde partij. Deze methode voor het realiseren van geschakeld vertrouwen vindt momenteel op meerdere plaatsen opgang als methodiek van beheersing. Als voorbeeld hiervan geldt de methodiek van system based auditing (SBA) zoals momenteel wordt vormgegeven in de context van douanes en toezichthouders op transport in logistieke ketens [CASSANDRA]. Om een eind-tot-eind risico assessment te kunnen doen op de logistieke ketens waarbij een groot aantal partijen betrokken is voor het uitvoeren van een deel van het transport, wordt daarbij gebruik gemaakt van het concept van ‘trusted traders’. Vanuit het perspectief van een douane of toezichthouder krijgt een ketenpartner deze status van ‘trusted trader’ wanneer deze voldoende maatregelen heeft geïmplementeerd om compliant te zijn aan de gestelde eisen m.b.t. bijvoorbeeld beveiliging. De status van ‘trusted trader’ kan eventueel worden gecertificeerd, leidend tot de status van ‘AEO’ (Authorized Economic Operator). Indien de (transport-)keten een toeleverancier bevat met de AEO-status, dan kan dit in het concept van system based auditing (SBA) voor de douane of toezichthouder voldoende motivatie zijn om deze toeleverancier op zodanige wijze te vertrouwen dat verdergaande eigen controle van hem (en alle eventueel achterliggende toeleveranciers) niet meer nodig is.

  Deze methode voor het realiseren van geschakeld vertrouwen op basis van controle of certificatie heeft een sterke relatie met de ketentypologie van ketensturing.

- *Op basis van gelijkwaardigheid en afspraken*

  Kenmerkend hiervoor is dat de betrouwbaarheid van de ketenpartner niet wordt afgedwongen middels een gezagsrelatie maar plaatsvindt op basis van gelijkwaardigheid. Deze gelijkwaardigheid kan worden bestendigd middels het maken van afspraken in de vorm van bijvoorbeeld een convenant. Van een dergelijke vrijwillig gesloten overeenkomst kan de nakoming niet worden afgedwongen.

Een voorbeeld van deze wijze van verkrijgen van betrouwbaarheid is het initiatief van 'Horizontaal Toezicht' zoals momenteel door de Nederlandse belastingdienst wordt nagestreefd. Met horizontaal toezicht wil de belastingdienst meer samenwerken met de fiscale dienstverlener en zijn cliënten. Wederzijds vertrouwen is het uitgangspunt om dit mogelijk te maken. De belastingdienst verbindt zich om snel een standpunt in te nemen met begrip voor commerciële belangen en termijnen. De ondernemer zorgt dat zijn fiscale processen op orde zijn en hij eventuele vraagstukken met de belastingdienst vooraf bespreekt. Uitgebreide controle achteraf is hierdoor in beginsel niet meer nodig. Wel kan een steekproef plaatsvinden door de belastingdienst, m.n. gericht op de fiscale dienstverlener. Voor het realiseren van horizontaal toezicht sluit de Belastingdienst convenanten met dergelijke fiscaal dienstverleners. Horizontaal toezicht zorgt ervoor dat de Belastingdienst het traditionele toezicht (de controle) gerichter in kan zetten bij die ondernemers waar specifieke risico's spelen.

Vertrouwen staat in dit geval niet gelijk aan 'blind vertrouwen' [KPMG]. Het representeert een 'middenweg, die ook wel 'ontwikkeld vertrouwen' of 'geïnformeerd vertrouwen' wordt genoemd: vertrouwen dat is gerechtvaardigd op grond van ervaringen of informatie.

Deze methode voor het realiseren van geschakeld vertrouwen op basis van gelijkwaardigheid en afspraken heeft een sterke relatie met de ketentypologie van ketenafstemming.

- *Op basis van eigen vaststelling*

  In de gevallen waarin geschakeld vertrouwen niet kan worden verkregen door één van beide methodes zoals boven beschreven zal een ketenpartner terugvallen op zijn eigen methodiek voor het vaststellen van (de mate van) betrouwbaarheid van vertrouwen.

  Deze methode voor het realiseren van geschakeld vertrouwen op basis van eigen vaststelling heeft een sterke relatie met de ketentypologie van ketenkoppeling.

De trust audit met haar normatiek zoals beschreven in dit referaat kan worden gebruikt om vast te stellen of (en welke vorm van en voor welke ketenpartners) geschakeld vertrouwen voor een specifieke ICT-keten gerechtvaardigd is. Daar waar als uitkomst van de trust audit geschakeld vertrouwen gerechtvaardigd blijkt, kunnen verdere controle maatregelen worden ingeperkt. De trust audit draagt op deze wijze bij aan zowel het vaststellen van de mate van kwaliteitsbeheersing van de ICT-keten als aan het inperken van aanvullende controles.

4.4 De trust audit t.b.v. risico assessment in de ICT-keten

In de methodiek van een 'top-down beoordeling' voor het uitvoeren van een controle op de robuustheid van een ICT-keten (zoals toegelicht in paragraaf 4.1), kan een trust audit als onderdeel van een risico-assessment op de robuustheid van de ICT-keten bijdragen aan het bepalen van de scope van de meest relevante te onderzoeken aspecten en daarmee de benodigde effort voor het uitvoeren van het onderzoek aanzienlijk

beperken. De trust audit kan hierbij als onderdeel van de risico-assessment een rol vervullen in het identificeren van risicogebieden en/of risico onderwerpen in de ICT-keten.

In deze paragraaf wordt de rol van de trust audit als onderdeel van een risico-assessment verder uitgewerkt op twee onderdelen:

- de trust audit als onderdeel van risico assessment in de ICT-keten,
- de trust audit voor het beheersen en beheren van risico's in ICT-ketens.

4.4.1 De trust audit als onderdeel van risico assessment in de ICT-keten

Een risico-assessment op de robuustheid van de ICT-keten kan bijdragen aan de scoping van de meest relevante te onderzoeken aspecten en de benodigde effort voor het uitvoeren van het onderzoek aanzienlijk beperken. De trust audit kan hierbij een rol vervullen in het identificeren van risicogebieden en/of risico onderwerpen in de ICT-keten door het vaststellen of er in voldoende mate kan worden vertrouwd op ketenpartners, bijvoorbeeld voor het realiseren van robuustheid van een ICT-keten. De toegevoegde waarde van de trust audit is daarbij het grootst bij de delen van de ICT-keten waarvoor geen directe invloed op de wijze van implementeren kan worden uitgeoefend.

Conform de aanpak van een risico assessment zoals die normaliter binnen een organisatie wordt uitgevoerd, onderscheiden we een aantal stappen voor het uitvoeren van een risico assessment in de ICT-keten met daarin de rol van de trust audit geborgd, zie Tabel 1.

Tabel 1: Stappen van een risico assessment proces in een ICT-keten met daarin de rol van de trust audit.

Stap 1 en stap 2 geven samen een beeld (de behoefte) voor welk deel van de keten er nog aanvullende risico assessment stappen nodig zijn om de robuustheid vast te stellen.

4.4.2 De trust audit voor het beheersen en beheren van risico's in ICT-ketens

De trust audit kan een rol spelen in de methode van voor het bepalen van de (mate van) controle over de robuustheid zoals eerder beschreven in [BASTIAANSEN1]. Deze methode staat bekend onder de naam 'El Metodo'. In deze paragraaf wordt deze methode (middels citatie) kort beschreven en wordt de rol van trust audits hierin benoemd.

De methodiek 'El Metodo' maakt gebruik van het concept van gescoopt risico management [JOOSTEN1]. Het uitgangspunt is dat de mate van controle over de robuustheid van een ICT-keten wordt bepaald vanuit de scope van de ketenverantwoordelijke.

Ter illustratie hiervan beschouwen we de keten van een chipkaart exploitant, waarin winkeliers klant zijn en chipkaartfunctionaliteit van die exploitant afnemen. De winkeliers verwachten van de exploitant onder meer dat de chipkaart terminals, de achterliggende systemen en de communicatie daartussen altijd werkt. De exploitant heeft zich hiertoe (contractueel) verplicht en zal om aan die verplichtingen te voldoen, zelf weer verwachtingen koesteren ten aan zien van zijn toeleveranciers (voor bijvoorbeeld de communicatie, het gestolen chipkaart register en financiële functies).

Figuur 6 laat zien dat de verwachting van de ene partij (ten aanzien van een andere partij), verplichtingen voor die andere partij worden (ten aanzien van de ene partij). De chipkaart exploitant (ketenverantwoordelijke) is verantwoordelijk voor het maken van afspraken met toeleverende partijen (communicatie provider en financiële instelling) voor de benodigde functionaliteit en het regisseren van alle interne en externe afspraken die maken dat hij zijn eigen functionaliteiten kan leveren en zijn verplichtingen nakomen.

Figuur 6: Verwachtingen en verplichting voor een chipkaart exploitant.

Om in controle te blijven over de robuustheid van de keten, zal de chipkaart exploitant moeten bepalen:

- hoe belangrijk elk van de toegeleverde functionaliteiten is voor de gehele dienst; d.w.z. wat is de impact bij uitval, en
- in welke mate hij erop vertrouwt dat de toeleverende partij haar afspraken nakomt, i.e., wat de 'trustscore' is voor de toeleverende partij.

De gedachte hierachter is dat als een toeleverende partij in gebreke blijft, het gevolg hiervan zou kunnen zijn dat ook de ketenverantwoordelijke zelf niet langer in staat is zijn verplichtingen na te komen, terwijl zijn klanten

geen genoegen zullen nemen met een verwijzing naar de subleverancier. Een winkelier die geen gebruik kan maken van de chipkaart, is immers niet geholpen als de chipkaart exploitant de verantwoordelijkheid voor een verstoring neerlegt bij de communicatie provider.

Indien de functionaliteit zeer belangrijk is of dat er onvoldoende vertrouwen is in de toeleverancier, dan zal de ketenverantwoordelijke zelf contingentiemaatregelen moeten nemen zoals het afnemen van communicatiediensten bij een tweede provider of het plaatsen van mobiele chipkaart terminals als backup.

Om inzicht te krijgen in de mate van controle over robuustheid maakt de methodiek 'El Metodo' gebruik van het concept van gescoopt risico management [JOOSTEN1]. Hierbij vult de ketenverantwoordelijke een risicomatrix in, zoals weergegeven in Figuur 7. Deze matrix bevat een overzicht van de verplichtingen (kolom Verplichtingen[i]) en verwachtingen (rij Verwachtingen[j]), gegroepeerd volgens de partijen tegenover wie deze verplichtingen en verwachtingen gelden. Per verplichting O wordt de impact van het niet nakomen van deze verplichting weergegeven met scores 'L', 'M' en 'H' in de kolom Impact[i]. In een cel geeft de afhankelijkheidscoëfficiënt aan in welke mate de verwachting (kolom) van belang is voor het waarmaken van de verplichting (rij). Verder geeft de ketenverantwoordelijke per verwachting E aan in hoeverre hij erop vertrouwt dat de toeleverancier deze verwachting (die voor de toeleverancier een verplichting is), gaat nakomen. De figuur laat dat zien middels trustscores 'L', 'M' en 'H' onder elke verwachting in de rij Trustscore[j]. Per verplichting wordt op basis van de afhankelijkheidscoëfficiënten en trustscores de kans op het niet nakomen van deze verplichting berekend in termen van de scores 'L', 'M' en 'H', zie kolom Kans[i]. Nu kan per verplichting het risico worden berekend op basis van kans en impact. De figuur toont dit middels scores 'L', 'M' en 'H' in de kolom Risico[i]. Indien een risico hoog uitkomt, heeft de ketenverantwoordelijk te weinig controle en zal hij contingentiemaatregelen moeten nemen, bijv. overgaan naar een betrouwbaardere toeleverancier.

risicomatrix voor robuustheid

					jezelf		een ander	
					E1	E2	E3	verwachting[j]
verplichting[i]	impact[i]	kans[i]	risico[i]	risico acceptabel?	H	M	L	trustscore[j]
O1	H	H	H	✘		+++	+++	
O2	M	L	L	✔	++	+		afhankelijkheids-coëfficiënt[i,j]
O3	L	H	M	✔		++	+++	

- ***trustscore***: *geeft voor elke verwachting (van jou) de mate van vertrouwen die jij hebt (jouw besluit!) in het waargemaakt worden van die verwachting*
- ***afhankelijkheidscoëfficiënt***: *relatieve bijdrage van verwachting aan het waarmaken van eigen verplichting ('+++', '++', '+', '0' of 'n.v.t./zwart')*
- *als jij **risico**[i] (= risico-inschatting horend bij **verplichting**[i]) acceptabel vindt, vink je dat bij die verplichting aan en ben je klaar (voor die verplichting tenminste)*

Figuur 7: Risicomatrix vanuit 1 scope.

Met 'El Metodo' kan dus niet alleen de mate worden vastgesteld waarin een ketenverantwoordelijke controle heeft over de robuustheid van die keten, maar heeft die ketenverantwoordelijke meteen een instrument in handen waarmee hij de (onacceptabel grote) risico's die hieruit voortvloeien kan beheren en mitigeren [JOOSTEN2].

Zoals bovenstaande beschrijving weergeeft, maakt 'El Metodo' maakt gebruik van trust scores, i.e. de mate van vertrouwen van de ketenverantwoordelijke (per verwachting) dat de toeleverancier deze verwachting gaat nakomen. Voor het (kwantitatief) bepalen van deze trust score is er een natuurlijke rol weggelegd voor de trust audit zoals beschreven in dit referaat. Middels weging van de normen en toetsen van de trust audit, kan de trust-score benodigd in 'El Metodo' worden vastgesteld.

4.5 De trust audit voor het kwantificeren van robuustheid van ICT-ketens

Naast het (in de vorige paragraaf beschreven) gebruik van de trust audit als instrument in een risico-assessment van ICT-ketens, kan de trust audit ook een rol vervullen ten behoeve van het kwantificeren van robuustheid van ICT-ketens.

In de volgende subparagrafen wordt het kwantificeren van robuustheid van ICT-ketens op een tweetal aspecten verder uitgewerkt, tezamen met de rol die de trust audit daarbij kan vervullen. Deze aspecten voor het kwantificeren van robuustheid van ICT-ketens zijn:

- De trust audit voor het vaststellen van de mate van controle over de robuustheid in ICT-ketens.
- De trust audit als input voor ICT-keten performance berekeningen.

4.5.1 De trust audit voor het vaststellen van de mate van controle over de robuustheid in ICT-ketens

In een ICT-keten is een ketenverantwoordelijke (indien überhaupt benoemd) in steeds grotere mate afhankelijk van toeleverende partijen waar hij zelf geen volledige controle over heeft, maar die desondanks wel van vitaal belang zijn voor het correct functioneren van "zijn" keten. Het is daarom voor de kwaliteit van de keten zeer belangrijk de keten zo goed mogelijk te organiseren, afspraken te maken over de (kwaliteit van) de dienstverlening van andere partijen en daarbij de kwaliteit over de gehele keten als leidraad te beschouwen. Behalve op SLA's zelf, zal de ketenverantwoordelijk ook een beeld moeten vormen in hoeverre hij verwacht dat de derde partij eraan voldoet.

Dit onderwerp hebben we eerder geadresseerd in [BASTIAANSEN1]. Voor het vaststellen van de mate van controle over de robuustheid van een ICT-keten zijn aanvullende criteria nodig. Deze criteria moeten ook nog eens (objectief) getoetst kunnen worden. In [BASTIAANSEN1] hebben we daarom een initiële set van criteria voor het vaststellen van de mate van controle over de robuustheid van een ICT-keten geïdentificeerd. De criteria zijn geclassificeerd in vier categorieën, zoals weergegeven in Tabel 2.

categorie	beschrijving	criteria
bestuurbaarheid	De mate waarin de ICT-keten is vormgegeven zodat het überhaupt mogelijk is om controle over de robuustheid uit te oefenen.	• doelstelling vastgelegd • *afgebakend in omvang* • gemodulariseerd
regie	De wijze waarop de regie over (de robuustheid van) de ICT-keten wordt uitgeoefend. Daarbij maken we verder onderscheid in de subcategorie "Ketenregie" en in de subcategorie "Ketenafspraken (SLA's)".	**ketenregie** • verantwoordelijkheden toegewezen • *middelen beschikbaar gesteld* • uitvoering vormgegeven • verantwoording afgelegd **ketenafspraken (SLA's)** • robuustheidseisen opgenomen • verantwoordelijkheden benoemd • verantwoording afgelegd
maatregelen	De maatregelen die zijn getroffen om de (controle over de) robuustheid van de ICT-keten te borgen, met een onderscheid in "technische maatregelen" en "bestuurlijke maatregelen".	**technisch** • risicoprofielen opgesteld • *maatregelen getroffen* **bestuurlijk** • ketenbreed risico-analyses uitgevoerd • ketenbreed risico-management proces ingericht
betrouwbaarheid	Die betrouwbaarheid van de afspraken en maatregelen die genomen zijn, zowel binnen een organisatie als tussen de partijen in de keten.	• *vertrouwen* • toetsing

Tabel 2: Categorieën en criteria voor het vaststellen van de mate van beheersing over robuustheid van ICT-ketens.

De rechterkolom in Tabel 2 geeft een overzicht van criteria per categorie. Voor elk van de criteria is een set van toetsen opgesteld die kan worden gebruikt om het desbetreffende criterium te "scoren". Voor de overzichtelijkheid zijn deze toetsen niet in de tabel opgenomen. Wel is in de tabel middels het schuingedrukte lettertype aangegeven welke criteria (ondanks de bijbehorende toetsen) niet volledig objectief zijn te scoren, maar waarvoor een meer subjectieve professionele beoordeling nodig is, gestoeld op ervarings- en vergelijkingsfeiten.

De rechterkolom in de tabel is onder de categorie 'betrouwbaarheid' het criterium 'vertrouwen' weergegeven. Zoals de tabel laat zien met het schuingedrukte lettertype was ten tijde van het opstellen van het artikel de opinie dat het criterium 'vertrouwen' niet volledig objectief was te scoren. De trust audit zoals beschreven in dit referaat echter geeft hiervoor wel een instrument, en verbetert daarmee deze gehele methodiek voor de kwantificering van robuustheid van ICT-ketens.

Tot slot wordt opgemerkt dat het voor het vaststellen van de mate van controle over de robuustheid in ICT-ketens het nodig is om de criteria uit de tabel op een herhaalbare, recursieve, wijze toe te passen. De criteria zijn immers zowel van toepassing voor de systemen onder intern beheer van de "eigen" schakel als voor de externe schakels in de ICT-keten. Deze externe schakels zullen bovendien weer hun eigen toeleveranciers hebben. Om de methodiek voor het vaststellen van de mate van controle over de robuustheid in ICT-ketens ketenbreed toe te passen kan daarom gebruik worden gemaakt van de 'El Metodo' methode zoals beschreven in paragraaf 4.4.2.

4.5.2 De trust audit als input voor ICT-keten performance berekeningen

Voor het kwantitatief bepalen van de kwaliteit (bijvoorbeeld in termen van beschikbaarheid of response tijden) van complexe ICT-ketens zijn wiskundige modellen nodig. Dergelijke wiskundige modellen zijn inmiddels beschikbaar en worden nog steeds verbeterd. In deze modellen wordt de kwaliteit van de gehele ICT-keten bepaald op basis van de kwaliteit van de individuele schakels, in combinatie met de topologie van de ICT-keten (voor de topologie van de ICT-keten: zie ook appendix A). Dergelijke wiskundige modellen houden voor de kwaliteit niet alleen rekening met de kwantitatieve waarden voor de kwaliteitsaspecten van een ICT-dienst zoals bijvoorbeeld weergegeven in de SLA (beschikbaarheid, response tijd, ...) maar ook met de betrouwbaarheid daarvan, vaak weergegeven met de term 'reputatie', zie bijvoorbeeld [WANG]. Een overzicht uit de wetenschappelijke literatuur hoe het aspect 'reputatie' daarbij kan worden gemodelleerd, gemeten en toegepast is beschreven in [JOSANG]. Het moge duidelijk zijn dat de trust audit zoals uitgewerkt in dit referaat ook hier weer een goede rol kan vervullen in het kwantificeren van deze betrouwbaarheid.

Bovengenoemde wiskundige modellen worden daarbij bijvoorbeeld toegepast voor de kwantitatieve kwaliteitsanalyse van on-line transactie verwerkende systemen of van constellaties van web services, waarbij invloed kan worden uitgewisseld op de topologie en keuze voor individuele ICT-diensten op basis van orkestratie. In de huidige Nederlandse onderzoeksprojecten SEQUAL (SErvice optimization and QUALity [SEQUAL]) en TTISC (Towards Trustworthy ICT Service Chains [TTISC]) wordt (o.a.) gewerkt aan het verder uitdiepen van deze wiskundige modellen en het gebruik daarvan om een 'orchestrator' te ontwerpen die dynamisch kan kiezen tussen verschillende diensten en dienstaanbieders om een optimale dienstcompositie samen te stellen onder een gegeven criterium (geoptimaliseerde inkomsten onder voorgeschreven betrouwbaarheid van kwaliteit) [WORM].

Naast het kwantitatief bepalen van de kwaliteit, kunnen dergelijke modellen ook worden gebruikt om het ontwerp van een ICT-keten vorm te geven (zowel de topologie van de ICT-keten als de keuze voor specifieke dienstleveranciers die als schakel in de keten worden opgenomen) en voor het overall statistisch doorrekenen van de tolerantie (inclusief de betrouwbaarheid) van elk van de individuele schakels in de ICT-keten naar de kwaliteit van de ICT-keten in zijn geheel.

5. Normatiek voor trust audits

Dit hoofdstuk werkt de normatiek voor trust audits uit. Daarbij wordt eerst aandacht besteed aan het doel van de normatiek in trust audits (paragraaf 5.1). Dit wordt gevolgd door een beschouwing van inter-organisatorisch vertrouwen als basis voor de structuur van het normenkader voor trust audits (paragraaf 5.2). Een uitwerking van dit normenkader wordt gegeven in paragraaf 5.3. Dit hoofdstuk wordt afgesloten met een beschouwing op de weegfactoren waarmee de diversie normen uit de normatiek kunnen worden gewogen (paragraaf 5.4).

5.1 Doel van de normatiek in trust audits

Zoals al in paragraaf 1.3 benoemd, lijkt het instrument van een trust audit voor het vaststellen van de mate van “betrouwbaarheid van vertrouwen” op een interne tegenstrijdigheid. Vertrouwen gaat er toch juist over dat je niet alles controleert? Dit lijkt in tegenspraak met het doel van de audit, i.e. toch proberen een (op een objectieve wijze) een maat aan de betrouwbaarheid van dit vertrouwen te geven.

Desalniettemin duiden de toepassingen van het onderwerp van trust audits (zoals benoemd en uitgewerkt in hoofdstuk 4) op voldoende potentie voor de trust audit als instrument bij het beoordelen van de robuustheid van ICT-ketens.

Het doel van de normatiek in trust audits voor het beoordelen van de robuustheid van ICT-ketens is om de betrouwbaarheid van ketenpartners op een zo objectief mogelijke manier vast te stellen en de gevoelsmatige beleving uit te schakelen [ROSIELLE]. De kwaliteit van de normatiek wordt daarbij bepaald door de volledigheid hiervan en de mate waarin ze subjectiviteit in de beoordeling van de betrouwbaarheid van ketenpartners weghaalt.

5.2 Structuur van de normatiek, gebaseerd op inter-organisatorisch vertrouwen

Deze paragraaf geeft de structuur voor het normenkader van trust audits. Deze structuur is afgeleid van een typologie voor inter-organisatorisch vertrouwen. Subparagraaf 5.2.1 beschouwt (kort) het concept van inter-organisatorisch vertrouwen, waarna subparagraaf 5.2.1 de structuur van het normenkader aangeeft.

5.2.1 Inter-organisatorisch vertrouwen als basis

Inter-organisatorisch vertrouwen is het vertrouwen van ketenpartners in elkaar met betrekking tot het nakomen van de aan elkaar gestelde verwachtingen. De trust audit is een instrument om (de mate van) dit inter-organisatorisch vertrouwen te beoordelen en te kwantificeren.

Zoals aangegeven in [IIARESEARCH], heeft voorgaand onderzoek uitgewezen dat interpersoonlijk vertrouwen en inter-organisatorisch vertrouwen sterk aan elkaar gerelateerd zijn, maar dat de verbinding ertussen niet altijd volledig duidelijk is. Contacten tussen bedrijven zijn vaak interpersoonlijke contacten, of tussen kleine groepen van mensen. Daar staat tegenover dat organisaties ook een eigen imago en publieke beeldvorming hebben, ze ontwikkelen werkwijzen, processen en een cultuur die het gedrag van hun medewerkers en hun omgang met

externe contacten uniformeren. In die zin is er wel degelijk een verbinding met inter-organisatorisch vertrouwen.

Dit inter-organisatorisch vertrouwen wordt vaak beschouwd als een van de ondersteunende pilaren van organisaties die samenwerken in netwerken of ketens [SYDOW]. Hierbij wordt verondersteld dat inter-organisatorisch vertrouwen binnen ketens:

- bijdraagt aan de vorming van 'collectieve strategieën',
- de coördinatie van economische activiteiten faciliteert,
- de open uitwisseling van informatie en het inter-organisatorisch leereffect bevordert,
- het beheersen van inter-organisatorische conflicten vergemakkelijkt.

Daarom draagt inter-organisatorisch vertrouwen op een aanzienlijke wijze bij aan de reductie van transactie kosten, het creëren van mogelijkheden voor strategische samenwerking, het verbeteren van kwaliteit en stabiliteit van de operationele processen en systemen en het ondersteunen van organisatorische verandering.

5.2.2 Structuur van de normatiek

Sinds decennia wordt er in de literatuur aandacht besteed aan het belang van onderling vertrouwen voor het onderhouden van inter-organisatorische samenwerking. Zoals aangegeven in [SEPPANEN] is er echter nog geen eenduidig beeld over de wijze waarop dit vertrouwen gemodelleerd, geoperationaliseerd en gemeten kan worden. Verschillende wetenschappers en auteurs hebben hiervoor verschillende wijzen gehanteerd.

In dit referaat sluiten we voor de typologie van inter-organisatorisch vertrouwen aan bij een aanpak zoals eerder beschreven is voor andersoortige ketens (bijvoorbeeld voor voedselketens in [CANAVARI]). Deze aanpak maken we in dit referaat specifiek voor het onderwerp robuustheid van ICT-ketens.

De aanpak voor de typologie gaat uit van het perspectief van de afnemer van een ICT dienst, omdat de afnemer te maken heeft met informatie asymmetrie over de af te nemen dienst. Op het hoogste niveau maakt de typologie daarbij onderscheid in drie 'aspecten' voor het vertrouwen:

- de ICT-dienst,
- de dienstaanbieder,
- het marktsegment.

Het is op dit punt goed even stil te staan bij bovengenoemde driedeling in de typologie. De kern bij het beoordelen van de robuustheid van ICT-ketens is het kunnen vaststellen van de 'kwaliteit' van de wijze waarop de toeleverende ketenpartners hun dienstverlening hebben ingericht. Deze kwaliteitsaspecten betreffen zogenaamde 'niet-functionele' aspecten van de dienst. Formeel kun je zeggen dat deze aspecten door een

goede normatiek voor de ICT-dienst al worden afgedekt. Eigenlijk hoef je 'alleen maar' betrouwbaarheid van het aangeleverde product te hebben. Echter, omdat het uitgangspunt bij de trust audits is dat je dit niet (door kijken in de keuken van alle toeleveranciers) kunt vaststellen. Dit onderbouwt het gebruik van de aanvullende aspecten 'dienstaanbieder' en 'marktsegment' in de normatiek als indirecte methode om betrouwbaarheid van het product op robuustheidseigenschappen vast te stellen.

Bij het uitwerken van de normen op de drie bovengenoemde objecten wordt daarbij gekeken vanuit het perspectief of het vertrouwen in een ketenpartner als toeleverancier van ICT-diensten voldoende is om de robuustheid van de ICT-keten te kunnen borgen.

5.3 Uitwerking van de normatiek in normenkaders

In deze paragraaf wordt de structuur van de normatiek voor trust audits (zoals beschreven in de vorige paragraaf) uitgewerkt in normenkaders. Daartoe beschrijft subparagraaf 5.3.1 de wijze waarop de concrete normen worden geïdentificeerd binnen de structuur van de normatiek. Een totaaloverzicht van de normen voor elk van de aspecten de 'ICT-dienst', de 'dienstaanbieder' en het 'marktsegment' is opgenomen in subparagraaf 5.3.2. Een uitwerking van het normenkader voor elk van de drie aspecten wordt gegeven in subparagraaf 5.3.3.

5.3.1 Methodiek voor het identificeren van normen

Deze subparagraaf beschrijft de wijze waarop de concrete normen worden geïdentificeerd binnen de structuur voor het inrichten van het normenkader, i.e. voor elk van de drie 'aspecten' zoals benoemd in subparagraaf 5.3.1.

Voor het identificeren van de normen voor de trust audit is uitgegaan van een twee-staps aanpak.

- In de eerste stap ('bottom-up') zijn bestaande normen voor trust audits genomen en is gekeken welke van de normen daarin toepasbaar zijn voor trust audits in de context van robuustheid van ICT-ketens. Daarbij is ook bepaald tot welk van de drie 'aspecten' behoort, waarbij het niet is uitgesloten dat eenzelfde norm wordt toegekend aan meer dan één aspect. De bestaande normen voor trust audits die hierbij zijn meegenomen zijn de normen voor vertrouwen tussen bedrijven en de normen voor interpersoonlijk vertrouwen zoals weergegeven in Appendix B.

- In de tweede stap ('top-down') is de omgekeerde richting gevolgd. Voor elk van de drie 'aspecten' binnen de structuur voor het inrichten van het normenkader is geanalyseerd of de initiële set van normen (zoals volgend uit stap 1) voldoende het aspect afdekt, of dat er nog aanvullende normen per aspect nodig zijn. Middels deze tweede stap wordt volledigheid van het normenkader voor elk van de aspecten nagestreefd.

5.3.2 Totaaloverzicht over de normen voor de drie aspecten

Tabel 3 geeft een overzicht van de normen die voor elk van de aspecten de 'ICT-dienst', de 'dienstaanbieder' en het 'marktsegment' resulteren na het volgen van 2-staps proces zoals beschreven in de vorige subparagraaf. Binnen elk aspect is daarbij een verdere categorisering van de normen aangebracht.

De tabel geeft voor elk van de normen tevens weer of er een relatie is met een norm uit een van beide bestaande normenkaders zoals beschreven bij stap 1. Hierbij relateert de naamgeving 'B2B' en 'P2P' aan respectievelijk de normen voor vertrouwen tussen bedrijven (B2B: Business-to-Business) en de normen voor interpersoonlijk vertrouwen (P2P: Person-to-Person), met de nummering corresponderend met de nummering zoals gebruikt in de tabellen van Appendix B.

De ICT-dienst				**De dienstaanbieder**		
Dienstaanbod				**Leveranciersafhankelijkheid**		
- kwaliteit dienstbeschrijving - wijze van afspraakvorming		P2P.9		- functionele symmetrie: in afhankelijkheid van de dienstverlening tussen leverancier en afnemer	B2B.2	P2P.5,10
Dienstafhankelijkheid				- financiële afhankelijkheid: van de toeleverancier aan de afnemer van het volgens afspraak leveren van de dienst.	B2B.2	P2P.5,10
- waarde van de dienst voor afnemer - financiële compensatie aan afnemer bij niet nakomen van verplichtingen	B2B.8 B2B.7			- typologie: open (ad hoc en vluchtige) of gesloten (langdurige en stabiele) relatie		
Beoordeling van dienst				**Openheid**		
- historische reputatie van de dienst - onafhankelijke beoordelingen op ICT-dienst	B2B.5, 6			- transparantie m.b.t. operationele processen en incidenten	B2B.3	P2P.3,11
				- invloed van de afnemer op de dienstaanbieder	B2B.4	
				- realistische communicatie door dienstaanbieder		P2P.1,8
				- gericht op verbetering van dienstaanbieder		P2P.4,7
Het marktsegment				**Omvang van de infrastructuur**		
Toezicht				- aantal componenten in de infrastructuur	B2B.9	
- extern toezicht op marktsegment - intern toezicht binnen marktsegment				- aantal 'achterliggende' toeleveranciers van de infrastructuur	B2B.1	
Beoordeling van marktsegment				- kwetsbaarheid van de infrastructuur	B2B.10	
				Beoordeling van dienstaanbieder		
- historische reputatie van marktsegment - transparantie in marktsegment	B2B.5, 6 B2B.3			- historische reputatie van dienstaanbieder	B2B.5, 6	P2P.6,12
				- beoordelingen en audits op dienstaanbieder	B2B.6	
				- afspraken over geschakeld vertrouwen		P2P.13

Tabel 3: Normen voor elk van de drie 'aspecten' voor vertrouwen.

De tabel laat zien dat elk van de normen voor vertrouwen tussen bedrijven (B2B, zoals voorgesteld in appendix B.2) is gerelateerd aan tenminste één van de normen voor vertrouwen zoals voorgesteld dit referaat en opgesomd in Tabel 3. Omgekeerd geldt echter niet dat elk van de van de normen voor vertrouwen zoals voorgesteld dit referaat een corresponderende norm heeft voor vertrouwen tussen bedrijven zoals voorgesteld in appendix B.2. Dit geeft aan dat ons normenkader uitgebreider is. Dit was verwacht omdat ons normenkader meer specifiek gericht is op (en daardoor volledige is in) normen gericht op robuustheid voor ICT-ketens.

5.3.3 Uitwerking van de normen voor de verschillende aspecten

Voor elk van de drie 'aspecten' voor het vertrouwen (de 'ICT-dienst', de 'dienstaanbieder' en het 'marktsegment') geven de volgende subparagrafen een uitwerking van de normen zoals aangegeven in Tabel 3.

5.3.3.1 Normen voor het aspect 'ICT-dienst'

Tabel 4 bevat de uitwerking van de normen voor het aspect 'ICT-dienst'.

De ICT dienst
Dienstaanbod De dienst die wordt aangeboden en de wijze waarop het aanbod tot stand is gekomen

Norm 1: Kwaliteit dienstbeschrijving
De kwaliteit van de dienstbeschrijving (inclusief SLA's) op de volgende aspecten:
• De functionele omschrijving van de geleverde dienst
• Volledigheid in beschrijving van niet-functionele (kwaliteits-) aspecten zoals:
  ➢ Beschikbaarheid, zowel in percentage per jaar als maximum aantal beschikbaarheidsincidenten per klasse (L/M/H)
  ➢ Recovery Time Objective (RTO)
  ➢ Recovery Point Objective (RPO)
  ➢ …
• Procedures in geval van incidenten of calamiteiten: incident management, escalatieprocedure, continuïteit management

Norm 2: Wijze van afspraakvorming De wijze van afspraakvorming voorafgaand aan het operationeel maken van koppelingen met toeleverancier, waaronder: • het niveau, de kwaliteit en het vertrouwen van intermenselijk contact bij afspraakvorming, • de rol van (en mate van) niet-functionele (kwaliteits-) aspecten bij de afspraakvorming. Hier wordt opgemerkt dat met moderne IT-ondersteuning (bijvoorbeeld Web Service technologie met automatische discovery en interconnectie van diensten) het niet altijd meer nodig is om persoonlijk contact met toeleveranciers te hebben om tot afspraakvorming te komen.
Dienstafhankelijkheid De waarde die het nakomen van de afspraken van de dienst door de leverancier heeft voor de afnemer
Norm 1: Waarde van de dienst voor afnemer De waarde die de afhankelijkheid van de dienst vertegenwoordigt voor de afnemer van de ICT-dienst. De waarde van de afhankelijkheid van de dienst wordt (mede) bepaald door: • financiële opbrengst voldoende om het risico van het gestelde vertrouwen te compenseren • impact op de eigen dienstverlening bij het niet nakomen van de afspraken, • interne maatregelen tegen het niet nakomen van de afspraken,

	• beschikbaarheid van alternatieven voor de dienst.
	Norm 2: Financiële compensatie aan afnemer bij niet nakomen van verplichtingen Het niveau van de financiële compensatie die is afgesproken met de leverancier in het geval van het niet nakomen van de afspraken en de mate waarin deze financiële compensatie genoegdoening geeft aan de afnemer in het geval dit zich daadwerkelijk voordoet.
	Beoordeling van de dienst De betrouwbaarheid van de ICT-dienst zoals historisch gebleken of beoordeeld door onafhankelijke partijen
	Norm 1: Historische reputatie van de dienst De historisch gebleken betrouwbaarheid van de ICT-dienst met betrekking tot het (niet) nakomen van de afspraken: incidenten, compromittatie of corruptie van de ICT-dienst. Dit historisch gedrag kan een indicatie geven over het toekomstig gedrag.
	Norm 2: Onafhankelijke beoordelingen op ICT-dienst Verklaring door een onafhankelijke partij over de kwaliteit van de dienst. De onafhankelijke mededelingen kunnen een informeel karakter hebben (bijvoorbeeld een review op een vergelijkende web pagina) of een formeel karakter hebben (bijvoorbeeld een Third Party Mededeling (TPM) door onafhankelijke auditor of accountant).

Tabel 4: Uitwerking van de normen voor het aspect 'ICT-dienst'.

5.3.3.2 Normen voor het aspect 'dienstaanbieder'

Tabel 5 bevat de uitwerking van de normen voor het aspect 'dienstaanbieder'.

De dienstaanbieder	
	Leveranciersafhankelijkheid Het belang dat het nakomen van de afspraken van de dienst vertegenwoordigt voor de leverancier hiervan
	Norm 1: Functionele symmetrie: in afhankelijkheid van de dienstverlening tussen leverancier en afnemer De symmetrie in afhankelijkheid van de dienstverlening tussen leverancier en afnemer. Niet alleen is de afnemer voor het verlenen van zijn dienstverlening afhankelijk van de toeleverancier. Het omgekeerde kan ook het geval zijn; de toeleverancier is op een vergelijkbare wijze afhankelijk van de afnemer. Deze situatie kan zich m.n. voordoen in ICT-ketens met een 'geschakelde topologie (zie appendix A.4)
	Norm 2: Financiële afhankelijkheid: van de toeleverancier aan de afnemer van het volgens afspraak leveren van de dienst De financiële afhankelijkheid van de toeleverancier aan de afnemer van het volgens afspraak leveren van de dienst. Indien dergelijke (financiële) afhankelijkheid bestaat, dan zal de toeleverancier in hogere mate geneigd zijn rekening te houden met de gevolgen van het schenden van het vertrouwen en het niet nakomen van de afspraken.

Norm 3: Typologie: open (ad hoc en vluchtige) of gesloten (langdurige en stabiele) relatie

De dynamiek van de relatie met de toeleverancier (zie appendix A.2):

- open relatie: ad hoc en vluchtige relatie met meerdere alternatieve dienstaanbieders,
- gesloten relatie: langdurige en stabiele relatie op basis van contractafspraken.

Openheid

De mate waarin de toeleverancier eerlijk en volledig communiceert over de implementatie en werkt aan verbetering, ook als hij daarvoor zijn eigen trots opzij moet zetten.

Norm 1: Transparantie m.b.t. operationele processen en incidenten

De mate waarin met de toeleverancier op zichtbare en open wijze wordt gecommuniceerd over de operationele, de dienstverlening, de processen en de incidenten.

Norm 2: Invloed van de afnemer op de dienstaanbieder

De mate van invloed die de afnemer kan uitoefenen op de toeleverancier.

Dit aspect heeft een relatie met het criterium 'invloed in ICT-ketens) van de typologie van de ICT-keten waarin de afnemer en toeleverancier als ketenpartners participeren (zie appendix A.3). Bij veel ICT-ketens is deze invloed beperkt en is de relatie gebaseerd op de afspraken in een dienstbeschrijving met bijbehorende SLA, i.e. het typ 'ketenkoppeling'.

Norm 3: Realistische communicatie door dienstaanbieder

De spelende zaken op open en realistische wijze bespreekbaar maken.

De essentie hierbij is dat de er niet om de echt belangrijke zaken in de communicatie tussen de afnemer en de toeleverancier wordt heen gedraaid.

Norm 4: Gericht op verbetering van dienstaanbieder

De toeleverancier is gericht op herstel van fouten en verbetering van competenties.

Omvang van de infrastructuur

De implementatie van dienstverlening door de toeleverancier is voor hem 'behapbaar'.

Norm 1: Aantal componenten in de infrastructuur

Het aantal componenten dat de toeleverancier nodig heeft om de ICT-dienst te leveren.

Het vertrouwen in de dienstverlening van een toeleverancier hangt samen met de omvang van de dienstverlening, in termen van het aantal componenten dat er bij de realisatie daarvan betrokken is, ofwel de 'behapbaarheid'. Is de omvang van de implementatie bij de toeleverancier van voldoende behapbaarheid voor een realistisch vertrouwen in het correct functioneren daarvan? Dit is niet beperkt tot de hardware / computers alleen. Het betreft ook de software, de data, de stroomvoorziening, de gebruikersinvoer, etc.

Norm 2: Aantal 'achterliggende' toeleveranciers van de infrastructuur

Het aantal 'achterliggende' toeleveranciers waarvan een toeleverancier zelf weer afhankelijk is om de ICT-dienst te leveren.

Dergelijke 'achterliggende' toeleveranciers zijn voor de afnemen in het algemeen niet zichtbaar. Dit geldt ook voor de afspraken met

	betrekking tot de kwaliteit van de dienstverlening die de directe toeleverancier met dergelijke 'achterliggende' toeleveranciers heeft gemaakt. Indien dit een groot aantal achterliggende 'achterliggende' toeleveranciers betreft komt dit het vertrouwen niet ten goede.
	Norm 3: Kwetsbaarheid van de infrastructuur De mate van veiligheid van de implementatie van de dienstverlening door de toeleverancier. De kwetsbaarheid betreft de balans tussen enerzijds de mate van (elektronische) openstelling van de implementatie aan de buitenwereld (bijvoorbeeld via het Internet met al haar dreigingen) en anderzijds het niveau van beveiligingsmaatregelen dat door de toeleverancier is getroffen.
	Beoordeling van de dienstaanbieder De betrouwbaarheid van de dienstaanbieder zoals historisch gebleken, beoordeeld door onafhankelijke partijen of zelfverklaard door toeleverancier.
	Norm 1: Historische reputatie van dienstaanbieder De historisch gebleken betrouwbaarheid van de dienstaanbieder met betrekking tot het (niet) nakomen van de afspraken: en incidenten. Dit historisch gedrag kan een indicatie geven over het toekomstig gedrag. Niet alleen absolute aantallen van historische incidenten zijn daarbij van belang, maar ook de frequentie en eventuele toe- of afname daarvan.
	Norm 2: Beoordelingen en audits op dienstaanbieder Verklaring door een onafhankelijke partij over de kwaliteit van de dienstaanbieder. De onafhankelijke mededelingen kunnen een informeel karakter hebben (bijvoorbeeld een review op een vergelijkende web pagina) of een formeel karakter hebben (bijvoorbeeld een Third Party Mededeling (TPM) door onafhankelijke auditor of accountant).
	Norm 3: Afspraken over geschakeld vertrouwen Bereidheid van toeleverancier om garant te staan voor kwaliteit, ook van 'achterliggende' toeleveranciers. Voor een afnemer is het belangrijk dat hij zijn 'naaste' toeleveranciers kan vertrouwen. Als zijn 'naaste' toeleveranciers namelijk betrouwbaar zijn, dan kan de afnemer er vertrouwen in hebben dat deze het benodigde niveau van compenserende maatregelen heeft genomen tegen eventuele onbetrouwbaarheid van hun achterliggende toeleveranciers. Op deze wijze ontstaat een 'geschakelde keten van vertrouwen', waarbij ketenpartners kunnen bouwen op het vertrouwen dat ze hebben in hun naaste toeleveranciers, i.e. geschakeld vertrouwen (zie paragraaf 4.3).

Tabel 5: Uitwerking van de normen voor het aspect 'dienstaanbieder'.

5.3.3.3 Normen voor het aspect 'marktsegment'

Tabel 6 bevat de uitwerking van de normen voor het aspect 'marktsegment'.

Het marktsegment
Toezicht
Norm 1: Extern toezicht op marktsegment De mate waarin het marktsegment waarin de toeleverancier werkzaam is aan extern toezicht is onderworpen met betrekking tot de kwaliteit van haar dienstverlening. Dit kan bijvoorbeeld het geval zijn ten gevolge van wet- en regelgeving. Op compliance aan dergelijke wet- en regelgeving kan het marktsegment onder extern toezicht staan van onafhankelijke toezichthouders.
Norm 2: Intern toezicht binnen marktsegment De mate waarin binnen het marktsegment zelf afspraken zijn gemaakt of een cultuur is gecreëerd betrekking tot het nakomen door haar organisaties van de kwaliteit van haar dienstverlening. Dergelijk intern toezicht (zelfregulering) kan eventueel gepaard zijn met een vorm van certificatie. Het eerder genoemde voorbeeld van het concept van 'trusted traders' (met certificatie van de status van 'AEO' (Authorized Economic Operator). zie paragraaf 4.3.1) kan als voorbeeld hiervan binnen het marktsegment 'logistiek' worden beschouwd.
Beoordeling van het marktsegment De betrouwbaarheid van het marktsegment zoals historisch gebleken of inzichtelijk gemaakt
Norm 1: Historische reputatie van marktsegment De historisch gebleken betrouwbaarheid van het marktsegment met betrekking tot de cultuur, afspraken en controle over betrouwbaarheid van de organisaties betrokken bij haar dienstverlening. Dit historisch gedrag kan een indicatie geven over het toekomstig gedrag.
Norm 2: Transparantie in marktsegment De mate waarin over de organisaties binnen het marktsegment op zichtbare en open wijze wordt gecommuniceerd over de operationele organisaties, hun diensten, processen en incidenten. Deze zichtbare en open communicatie hoeft niet direct naar alle afnemers te zijn, dit kan ook indirect via derden. Het feit alleen dat bekend is dat er op zichtbare en open wijze wordt gecommuniceerd kan het vertrouwen al doen toenemen.

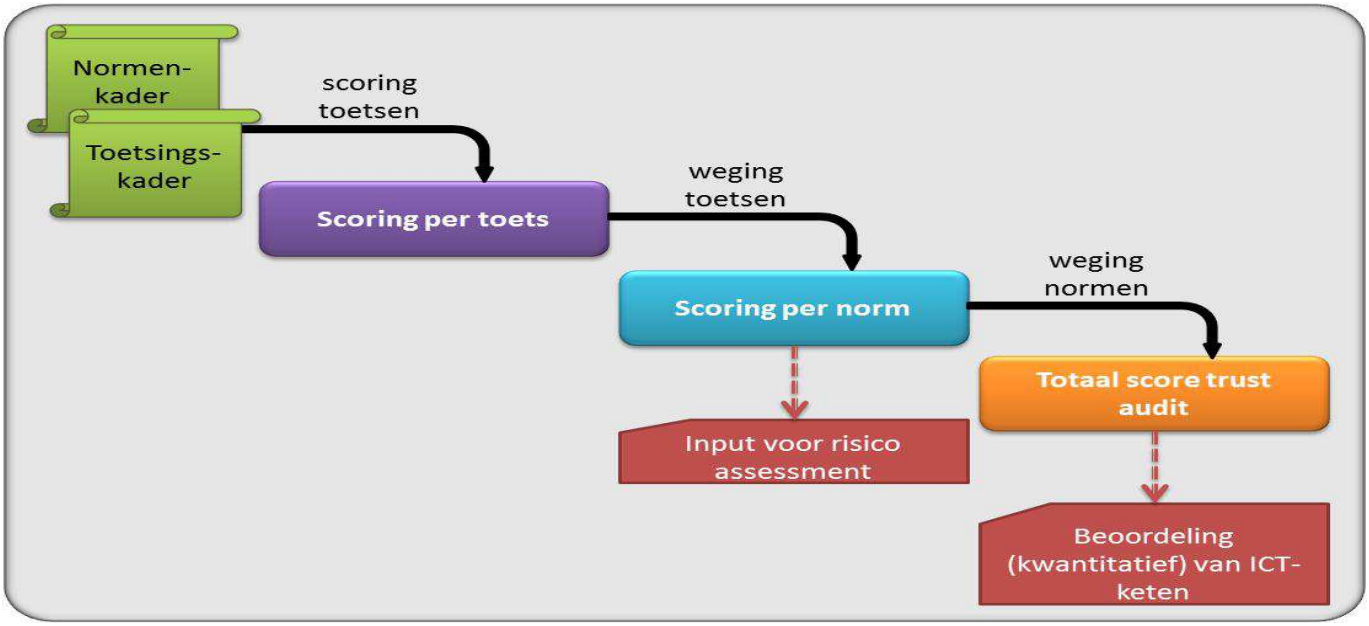
Tabel 6: Uitwerking van de normen voor het aspect 'marktsegment'.

5.4 Weging en scoring van de normen

In de vorige paragraaf zijn de (initiële) normenkaders gegeven voor de trust audit op de aspecten de ICT-dienst, de dienstaanbieder en het marktsegment. Om bij de uitvoering van een trust audit met dit normenkader tot een beoordeling te komen is het nodig om de individuele normen te scoren middels een afgeleid en SMART toetsingskader. Een dergelijk toetsingskader is buiten de scope van dit referaat. De scoring kan zowel op

kwalitatieve wijze (bijvoorbeeld met 'rood'-, 'geel'-, 'groen'-scores) als op kwantitatieve wijze (bijvoorbeeld een waarde op de schaal van 0 tot 10) worden gedaan.

Om op basis van een trust tot een algehele (kwantitatieve) beoordeling te komen van de robuustheid van ICT-ketens dienen zowel het toetsings- als normenkader te worden aangevuld met 'weging'. De weging per norm van de toetsen in het toetsingskader leidt tot een scoring per norm. De resultaten van deze scoring geeft inzicht in de mogelijke risicogebieden. De weging van de normen in het normenkader leidt vervolgens tot een (kwantitatieve) beoordeling op basis van de trust audit van de robuustheid van de algehele ICT-keten. Deze concatenatie van scoring en weging is grafisch weergegeven in Figuur 8.



Figuur 8: Concatenatie van scoring en weging bij de uitvoer van de trust audit.

Ook de wegingen van toetsen en normen kunnen zowel op kwalitatieve wijze (bijvoorbeeld met 'hoog'-, 'middel'-, 'laag'-scores) als op kwantitatieve wijze (bijvoorbeeld een waarde op de schaal van 0 tot 10) worden gedaan. De kwalitatieve wijze van weging en scoring sluit goed aan wanneer de trust audit wordt gebruikt voor het uitvoeren van een risico-assessment (paragraaf 4.3). De kwalitatieve wijze van weging en scoring is juist benodigd wanneer de trust audit wordt gebruikt voor het kwantificeren van de robuustheid van ICT-ketens (paragraaf 4.4).

Het is op deze plaats echter niet mogelijk een eenduidige kwantitatieve wegingsschaal van de toetsen en normen te geven. De reden hiervoor is dat de weging van de toetsen en de normen sterk afhankelijk is van de context waarin de trust audit wordt toegepast. Deze context (en daarmee de kwantificering van de weging) is bijvoorbeeld afhankelijk van de volgende aspecten:

- *Het onderwerp van robuustheid dat wordt beschouwd voor het uitvoeren van de trust audit.*

Als het onderwerp bijvoorbeeld beschikbaarheid betreft, dan is het aspect 'ICT-dienst' relatief belangrijk in de weging. Betreft het onderwerp incident management, dan hebben de processen en daarmee de het aspect 'dienstaanbieder' een grotere rol. Betreft het onderwerp compliance aan wet- en regelgeving, dan speelt ook het aspect 'marktsegment' een rol in de weging.

- *De typologie van de ICT-keten.*

  Bij open ketens worden bijvoorbeeld op dynamische wijze relaties tussen ketenpartners aangegaan. In dat geval is het aspect 'ICT-dienst' relatief belangrijk. Bij gesloten ketens worden vaak langdurigere en intensievere samenwerking aangegaan. In dat geval zullen de aspecten 'dienstaanbieder' en 'marktsegment' een grotere rol spelen in de weging.


trust

6. Conclusies en aanbevelingen

In dit referaat is de trust audit als instrument voor het vaststellen van de mate van vertrouwen in ketenpartners beschouwd, met de op de beoordeling van de robuustheid van ICT-ketens. Zowel de rollen die trust audits kunnen vervullen als instrument voor ICT-ketenbeheersing, als de normatiek voor het uitvoeren van trust audits zijn beschouwd.

Dit hoofdstuk bevat de afsluitende conclusies (paragraaf 6.1) en aanbevelingen van het onderzoek verricht voor het referaat (paragraaf 6.2).

6.1 Conclusies

Uit het onderzoek naar de trust audit voor dit referaat kunnen de volgende conclusies worden getrokken.

- Op een aantal terreinen voor het vaststellen van robuustheid van ICT-ketens kunnen trust audits een nuttige rol vervullen. De rollen die als zodanig in dit referaat zijn onderkend en uitgewerkt zijn:
    - Het bouwen op geschakeld vertrouwen tussen ketenpartners.
    - Het bijdragen aan een risico assessment van de ICT-keten.
    - Het bijdragen aan het kwantificeren van de mate van robuustheid van een ICT-keten.
- Trust audits kennen ook hun beperkingen. Een trust audit doet geen strikte controle op de implementatie van de ICT-omgeving binnen individuele ketenpartners. De trust audit is dan ook niet een instrument waarmee ‘positive assurance’ kan worden verkregen met betrekking tot de robuustheid van ICT-ketens (vanuit ketenperspectief) of van individuele ketenpartners (vanuit partnerperspectief). De rol van de trust audit is inherent beperkt tot het kunnen bijdragen aan het afgeven van ‘negative assurance’.

  Het wordt hierbij opgemerkt dat ook het ‘omgekeerde’ niet het geval is: vanuit de trust audit kun je ook niet zeggen dat iets niet voldoet. Er wordt namelijk geen strikte controle op de implementatie van de ICT-omgeving uitgevoerd.

6.2 Aanbevelingen

De aanbevelingen richten zich op twee aspecten:

- Aanbevelingen voor het verder ontwikkelen van de trust audits voor het beoordelen van robuustheid van ICT-ketens zoals beschreven in dit referaat. Deze verdere uitwerking kan op de volgende punten:
    - Het opstellen en uitwerken van een toetsingskader voor de normatiek van trust audits zoals beschreven in hoofdstuk 5.

- Het beproeven van de trust audit als methodiek in een aantal representatieve ICT-ketens. Naast de theoretische beschrijving in dit referaat, levert dit inzicht in de waarde en toepasbaarheid van het gebruik van trust audits in real-life ICT-ketens.

- Het uitwerken van de trust audits voor rollen in het beoordelen van robuustheid van ICT-ketens, aanvullend aan de rollen benoemd en beschreven in hoofdstuk 4. Hierbij kan bijvoorbeeld gedacht worden aan rollen van de trust audit in (statische) aanbesteding- en procuratietrajecten voor samenwerkingsverbanden, of (nog verder weg in de tijd) als onderdeel van de automatische discovery en integratie van diensten en dienstpartners in dynamische, service-gerichte (Engelse terminologie: 'service oriented') ICT-ketens.

- Aanbevelingen voor het uitbreiden van de scope van de trust audits buiten de scope van het beoordelen van robuustheid van ICT-ketens zoals beschreven in dit referaat. Deze scope uitbreiding kan bijvoorbeeld op de volgende terreinen:

  - Aspecten op het terrein van de strategische beheersing van ICT-ketens (de 'bovenste' laag uit het C^4-model voor ketenbeheersing, zoals weergegeven in Figuur 3). Hierbij kan bijvoorbeeld gedacht worden aan de rol van trust audits in het beoordelen van capabilities van ICT-ketenpartners voor het gezamenlijk in ketenverband strategisch uitnutten en optimaliseren van de business waarde van ICT. Momenteel is dit (intra-organisatorisch) vormgegeven door het IT Capability Maturity Framework raamwerk van het Innovation Value Institute (IVI) [IT-CMF] [CURLEY] Aan uitbreiding hiervan naar (intra-organisatorisch) ICT-ketenverband wordt momenteel door het IVI (Innovation Value Institute) in samenwerking met TNO gewerkt.

  - Aspecten op het terrein van de ondersteunende processen voor de beheersing van ICT-ketens. Hierbij kan bijvoorbeeld worden gedacht aan de gezamenlijke afstemming, oefening en uitvoering in ketenverband van processen zoals incident management en business continuïteits-management.

7. Referenties

[BASTIAANSEN1] H. Bastiaansen, R. Joosten, E. Meeuwissen en F. Roijers: "*Hoe goed bent U in control over de robuustheid van uw ICT-keten?*", Informatie, Maart 2011, pp. 24 – 30.

[BASTIAANSEN2] H. Bastiaansen, E. Matthijssen en M. Schenk: "*Continuïteitsmanagement in vitale ICT-keteninfrastructuren vergt nieuwe bestuurlijke aanpak*", TIEM 2.0, Nummer 42, Najaar 2011, pp. 50 – 57.

[BASTIAANSEN3] H. Bastiaansen en Y. van Wijk: Concept artikel: "*Een model voor de beheersing en controle van ICT-ketens – Het Chain Content, Context & Control (C^4-) model*", in te dienen voor publicatie, met als optie het Norea tijdschrift 'de IT-Auditor', 2012. Ook opgenomen als Appendix C van dit referaat.

[BASTIAANSEN4] H. Bastiaansen, E. Matthijssen, B. Spitzer en M. Schenk: "*Continuïteitsmanagement in vitale ICT-keteninfrastructuren*", Best Practice Quarterly Review (BPQR), Jaargang 2, Nummer 4, Juli 2011, pp. 18 – 22.

[CANAVARI] M. Canavari., M. Fritz, G.J. Hofstede, A. Matopoulos en M. Vlachopoulou: "*The role of trust in the transition from traditional to electronic B2B relationships in agri-food chains*", Computers and Electronics in Agriculture 70, 2010, pp. 321–327.

[CASSANDRA] The EU FP7 project CASSANDRA, http://www.cassandra-project.eu.

[COVEY] S.M.R. Covey en R.R. Merrill: "*The Speed Of Trust: The One Thing That Changes Everything*", 2008, ISBN: 9781416549000.

[CURLEY] M. Curley, "*Managing information technology for business value – Practical Strategies for IT and business managers*", Intel Press, ISBN: 0-9717861-7-8.

[EDPAUDITOR1] A.J. van der Meer en L.G. Dirks, "Ketenauditing in de publieke sector, complex en daarom spannend!", De EDPAuditor nr. 3 2005.

[EDPAUDITOR2] A.J.M. de Bruijn, A.J. van der Meer, P.C.J. Nieuwenhuizen, M.C.M. Slot, B.J. van Staveren: "*Ketengovernance: ketensamenwerking binnen het publieke domein*". De EDP-Auditor nr. 2 2006.

[EDPAUDITOR3] A.J.M. de Bruijn, A.J. van der Meer, P.C.J. Nieuwenhuizen, M.C.M. Slot, B.J. van Staveren: "*Ketengovernance: startpunt voor keteninrichting en ketenauditing*", De EDP-Auditor nr. 1 2006.

[EDPAUDITOR4] R.J. Mollema en M.M.J.M. Welters: "*Vaktechnisch verantwoorde ketenaudits: optie of utopie?*", De EDP-Auditor nr. 3 2010.

[ENISA] ENISA – Network Resilience and Security: Challenges and Measures. December 2009. Available at: http://www.enisa.europa.eu/act/res/providers-measures/files/vwg-challenges-and-measures.

[FIELT] M. Fielt en H. de Smit: "*Meten en weten in de keten – IT-beheer in ketens vatbaar voor*

verbetering", IT Beheer Magazine, blz. 51-56, Oktober 2002.

[IIARESEARCH] IIA Research Report: "*Viewing Organizational Trust and Internal Auditing*", The Institute of Internal Auditors Dallas Chapter, 2003-2004 Research Paper, te downloaden op: http://www.theiia.org/research/research-reports/chapter-sponsored-research-list/?search=organizational trust.

[ISECOM] C. Rosielle: "*Trust Analysis*", ISECOM OSSTMM v3, , blz. 90-97, 2010.

[ISO] International Standard ISO/IEC 9126-1: "*Software engineering — Product quality — Part 1: Quality model*", First edition, 2001-06-15.

[IT-CMF] IT-CMF website: http://ivi.nuim.ie/itcmf.shtml

[JOOSTEN1] R. Joosten: "'*Gescoopt' Risico Management*", Informatiebeveiliging, Oktober 2010, pp. 12 – 17.

[JOOSTEN2] M. Hoeve, R. Joosten, E. Matthijssen, C. van der Weerdt en R. Wolthuis: "*El Metodo – Managing Risks in Value Chains*", Securing electronic business processes: highlights of the information security solutions Europe 2011 conference / ISSE 2011, Norbert Pohlmann (ed.) e.a., pp 214-223.

[JOSANG] A. Josang, R. Ismail en C. Boyd: "*A survey of trust and reputation systems for online service provision*", Decision Support Systems, 2007, 43(2): 618-644.

[KPMG] E. Roos Lindgreen, J. Strikwerda en N. Wielaard: "*Het nieuwe ondernemen – Het belang van vertrouwen voor de onderneming van de toekomst*", KPMG-uitgave, ISBN 978-90-6962-255-2.

[NOREA] NOREA keten audit publicaties, op: http://www.norea.nl/Norea/Regios+en+afdelingen/Kennisgroep+Zorg+en+IT/Werkgroep+Ketenauditing.aspx,

[QUINT] SERC: "*Kwaliteit van softwareprodukten – Praktijkervaringen met een kwaliteitsmodel*", 1996.

[RATNASINGAM1] P. Ratnasingam: "*Inter-Organizational Trust for Business to Business E-Commerce*", 2003, ISBN: 1-931777-75-6.

[RATNASINGAM2] P. Ratnasingam en P. Pavlou: "*Technology trust: The next value creator in B2B electronic commerce", Information Resources Management Association Conference*", Seattle, Washington, May 19th-22nd, 2002, pp. 889-894.

[RATNASINGAM3] P. Ratnasingam en P. Pavlou: "*Technology trust in inter-organizational electronic commerce*", Journal of Electronic Commerce in Organizations, vol. 1, Nr. 1, pp. 17-41, (Jan – Mar) 2003, Inaugural issue.

[ROSIELLE] C. Rosielle: "*Trust Audits*", Informatiebeveiliging, blz. 19-22, November 2010.

[SCHILDER] A. Schilder, H. Gortemaker, J. van Manen en J. Waardenburg: "*Moderne Accountantscontrole – de controle van de jaarrekening: risicoanalyse, interne beheersing en toegevoegde waarde*", derde herzien editie, SDU Uitgevers, ISBN-13: 978 90 395 19868.

[SEPPANEN] R. Seppänen, K. Blomqvist en S. Sundqvist: "*Measuring inter-organizational trust—a critical review of the empirical research in 1990–2003*", Industrial Marketing Management 36, 2007, pp. 249– 265.

[SEQUAL] IOP GenCom onderzoeksproject: "*SEQUAL (Service optimization and QUALity)*", http://www.agentschapnl.nl/content/project-service-optimization-and-quality-sequal.

[SYDOW] J. Sydow: "*Understanding the constitution of inter-organizational trust, Trust Within and Between Organizations*", 1998, Oxford: University Press.

[THIADENS] T. Thiadens: "*Sturing en organisatie van ICT-voorzieningen: de focus op vraaggestuurd leveren van ICT-voorzieningen*", ISBN: 9789087533069, Van Haren Publishing, 2e druk, 2008.

[TTISC] IIP onderzoeksproject: "*TTISC (Towards Trustworthy ICT Service Chains)*", ICT-regie innovatieplatform. http://www.ict2030.nl/IIP-Cooperation-Challenge.html.

[WANG] S. Wang, L. Zhang en L. Wang: "*A measurement approach of trust relations in web services*", Journal of Communication and Computer, Aug. 2009, Volume 6, No.8, pp. 9– 17.

[WORM] Worm, D., Berg, H. van den, Mei, R. van der, Zivkovic, M., "*Revenue Optimisation for ICT Service Chains under Availability Constraints*", to be submitted for publication.


trust

Appendix A: Typologie van ICT-ketens

De rol die vertrouwen en trust audits kunnen spelen in het beoordelen van ICT-ketens heeft een verband met het type relatie die rollen in de keten ten opzicht van elkaar vervullen en de wijze waarop deze relatie wordt ingevuld. We praten dan over de typologie van ICT-ketens.

De typologie van ICT-ketens is het onderwerp van deze appendix. Er is in de literatuur al een grote diversiteit aan publicaties gerelateerd aan dit onderwerp verschenen. Het doel van deze appendix is om een typologie van ICT-ketens aan te geven die goede bruikbaarheid heeft in het aangeven wat de rol van trust audits kan zijn in het beoordelen van de robuustheid van ICT-ketens.

A.1 Criteria voor de typologie van ICT-ketens

Het startpunt van een typologie vormen de criteria op basis waarvan je verschillende types van ICT-ketens van elkaar gaat onderscheiden. Voor de typologie van ICT-ketens zoals we in dit referaat hanteren we de volgende criteria voor het onderscheiden van ICT-ketens:

- de invloed in ICT-ketens,
- de dynamiek van ICT-ketens,
- de topologie van ICT-ketens.

Met betrekking tot dit drietal criteria *voor het onderscheiden van ICT-ketens* kunnen de volgende observaties worden gemaakt:

- *De criteria voor het onderscheiden van ICT-ketens zijn onderling onafhankelijk*

  Het wordt hierbij wel opgemerkt dat de criteria weliswaar *onderling onafhankelijk* zijn, maar dit neemt niet weg dat bepaalde combinaties in invulling per criterium aanzienlijk vaker zullen voorkomen dan anderen. Als voorbeeld hiervan kunnen we noemen dat voor dynamische ketens waarbij op ad-hoc wijze samenwerking tussen partijen in de ICT-keten wordt vormgegeven relatief slechts een zwakke mate van invloed op elkaar uitoefenen zal bestaan.

- *Deze set van criteria voor het onderscheiden van ICT-ketens vormt niet een 'volledige' set voor de typologie van ICT-ketens, maar is wel afdoende voor de scope van het referaat.*

  De aspecten die door de criteria zijn afgedekt omvatten respectievelijk: het niveau van interactie (invloed), de tijdsfactor (dynamiek) en de wijze van samenhang (topologie). De beide eerstgenoemde aspecten (invloed en dynamiek) hebben betrekking op de mate waarin ketenpartners kunnen worden vertrouwd (in termen van risico-analyse relateert dit aan de 'kans'). Het laatstgenoemde aspect (topologie) heeft betrekking op de gevolgen wanneer het vertrouwen wordt beschaamd ((in termen van

risico-analyse relateert dit aan de 'impact'). Gezamenlijk zijn zij daarmee afdoende voor de scope van het referaat omdat ze vanuit het perspectief van vertrouwen zowel kans als impact afdekken.

Deze set van criteria voor het onderscheiden van ICT-ketens vormt echter niet een 'volledige' set voor de typologie van ICT-ketens. Aanvullende criteria zijn bijvoorbeeld de omvang van de ICT-keten (in termen van aantal ketenpartners), de omvang van de ketenpartners, het belang van de ICT-keten, ….. Deze aanvullende criteria worden echter van minder belang voor het onderwerp van dit referaat beschouwd.

De volgende paragrafen geven een verdere uitwerking elk van bovengenoemde criteria. Voor een groot deel wordt daarbij voortgebouwd op de typologie van ICT-ketens zoals beschreven in [FIELT].

A.2 Criterium: dynamiek van ICT-ketens

In [TI] wordt een onderscheid gemaakt tussen open en gesloten ketens, als twee verschijningsvormen die kunnen worden onderkend binnen het criterium dat we in dit referaat aanduiden als de dynamiek van de ICT-ketens[2]:

- *Open ketens*

  Een open keten wordt gekarakteriseerd door wisselende actoren, vrije toegang, kortstondige relaties, verspreide en wisselende macht, een beperkte integratie en de situatie dat het bedrijfsbelang (een ketenentiteit) veelal prioriteit heeft boven het ketenbelang.

  Naar onze waarneming komen open ketens vooral voor in de private sector en veel minder vaak in de publieke sector. Open ketens kennen in veel gevallen meerdere spelers per functie in de keten.

  De verschillende spelers zoeken vooral optimalisatie in de één-op-één-relaties. Ketenoptimalisatie in open ketens wordt vooral nagestreefd met de nadruk op ontkoppeling van bedrijfsprocessen.

- *Gesloten ketens*

  Een gesloten keten daarentegen wordt gekarakteriseerd door een stabiel en bekend aantal actoren, langdurige relaties, het gegeven dat de macht veelal aan een paar grote 'spelers' is en verregaande integratie. Verder heeft het ketenbelang veelal prioriteit boven het individuele ketenentiteitbelang.

  Gesloten ketens zien wij veelvuldig (maar niet uitsluitend) voorkomen in de publieke sector, waar vooral wet- en regelgeving deze ketens vormgeeft. De private sector kent ook belangrijke gesloten ketens, in onder andere de distributie- en transportsector.

[2] De opgenomen omschrijving van open en gesloten ketens is een citaat uit [FIELT]

Gesloten ketens zoeken vooral naar optimalisatie over de keten heen. Ketenoptimalisatie wordt vooral nagestreefd met de nadruk op koppeling van bedrijfsprocessen. Langdurige relaties maken het mogelijk bedrijfsprocessen van de diverse spelers sterk te integreren.

A.3 Criterium: invloed in ICT-ketens

In [FIELT] wordt als criterium voor het onderscheiden van ICT-ketens de “mate van informatisering” van ICT-ketens gebruikt. Dit criterium onderscheidt types in de wijze waarop verschillende rollen in de ICT-keten toegang hebben tot elkaars informatiesystemen. Het artikel [FIELT] gebruikt dit onderscheid op basis van haar viewpoint “IT-beheer”. Hieraan rakend (maar met een ander viewpoint als uitgangspunt) wordt in [THIADENS] het criterium “Macht in de keten” gebruikt als basis voor een typologie.

In lijn met beide bovenstaande referenties, maken we in dit referaat gebruik van een variant op de genoemde criteria, te weten “invloed in ICT-ketens”. Dit criterium typeert de mate van onderlinge invloed en beïnvloeding tussen de ketenparners binnen een ICT-keten. Op basis van dit criterium worden de volgende drie karakteristieke typologieën onderscheiden:

- *Ketenkoppeling*

  Bij ketenkoppeling werken ketenpartners met elkaar samen op basis afspraken over hun koppelvlak, zonder daarbij afstemming te hebben over de geleverde functionaliteit of de (kwaliteit van) de technische implementatie. Deze situatie treedt bijvoorbeeld op wanneer diensten op dynamische wijze middels service oriëntatie worden afgenomen.

- *Ketenafstemming*

  Bij ketenafstemming stemmen ketenpartners wel de functionaliteit en de kwaliteit op elkaar af. Op basis van consensus kunnen daarbij beslissingen worden genomen. Een voorbeeld hiervan is de situatie waarin ketenpartners op basis van gedeeld belang met elkaar de kwaliteit van hun technische implementatie bespreken, risico’s en zwakheden identificeren en eventueel tot (technische of procesmatige) compenserende maatregelen besluiten zoals bijvoorbeeld in [BASTIAANSEN2] beschreven voor het kwaliteitsaspect continuïteitsmanagement. Als speciale uitingsvormen hiervan kunnen het afgeven van een Service Level Agreement (SLA) of een Third Party Mededeling (TPM) worden genoemd.

- *Ketensturing*

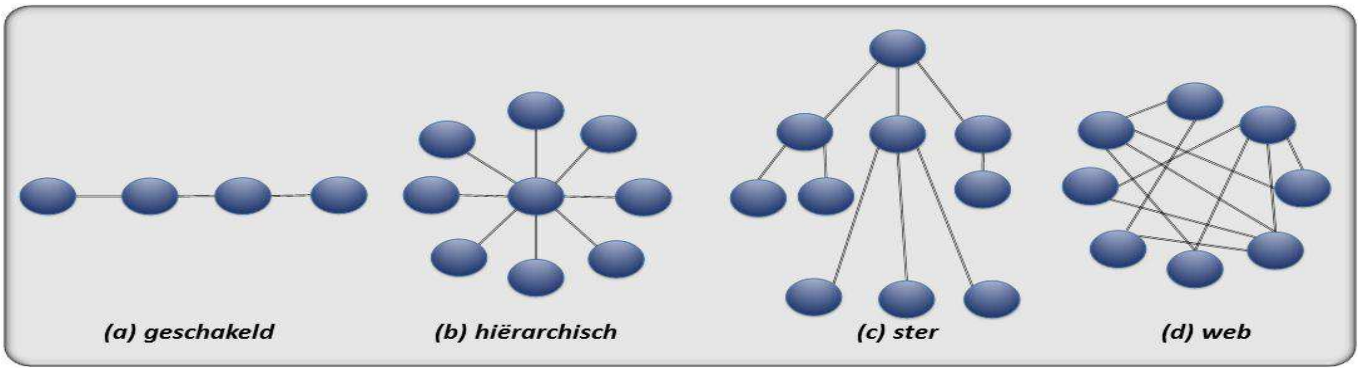
  Bij ketensturing is er sprake van een ketenpartner met voldoende overkoepelend gezag om eisen aan ketenpartners op te kunnen leggen over de wijze van invulling van hun ICT-voorzieningen. Dit zowel bijvoorbeeld doordat er een ketenpartner is met een dominante marktpositie of doordat er vanuit wet en regelgeving eisen worden opgelegd.

A.4 Criterium: topologie van ICT-ketens

Met betrekking tot de topologie van ICT-ketens onderkennen we de volgende opties, zoals ook bekend uit de traditionele literatuur en studies over topologieën van telecommunicatie netwerken:

- Geschakelde structuur
- Hiërarchische structuur (boom-structuur)
- Ster-structuur
- Web-structuur (vermaasde structuur)

Deze vier structuren zijn grafisch weergegeven in Figuur 9.



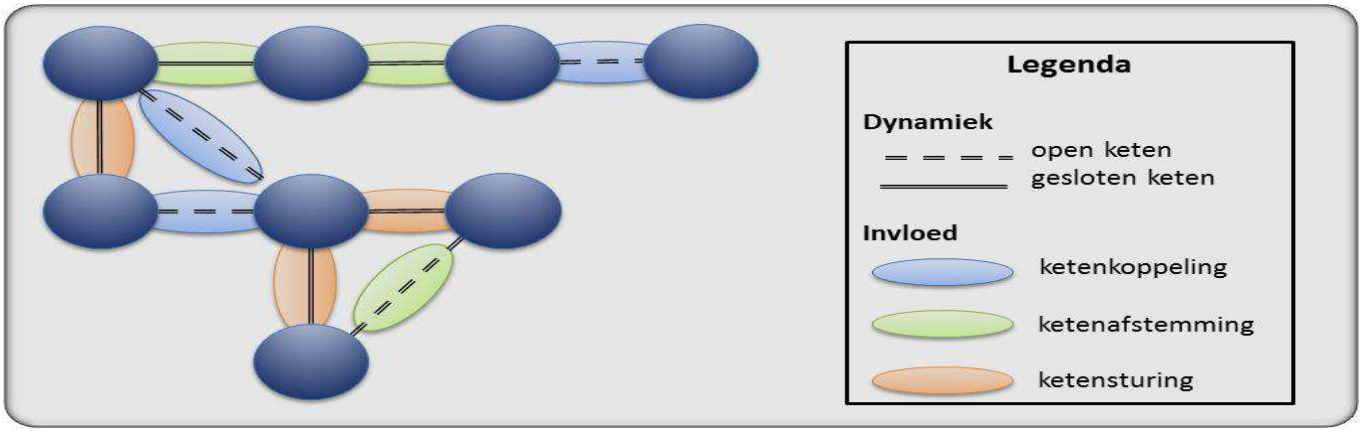
Figuur 9: Topologieën van ICT-ketens.

De topologie van een ICT-keten geeft inzicht in de gevolgen van het onbetrouwbaar blijken van een specifieke ketenpartner, bijvoorbeeld met betrekking tot beschikbaarheid. De topologie geeft daarbij aan welke ketenpartners hierdoor worden geraakt en eventueel welke (achterliggende' ketentpartners wegvallen. In termen van risico-analyse relateert dit aan de 'impact' van een incident.

Daarnaast kan de topologie inzicht geven in 'alternatieve routes' door de keten bij het wegvallen van één van de ketenpartners. In termen van risico-analyse relateert dit aan de 'maatregel' voor het mitigeren van een incident.

A.5 Hybride ICT-ketens

In bovenstaande paragrafen is een drietal criteria gegeven waarop types van ICT-ketens zich onderscheiden. Echter, in het algemeen kunnen specifieke ICT-ketens niet worden gekarakteriseerd met een één-éénduidige keuze van opties uit bovenstaande criteria. Specifieke ICT-ketens zullen (voor delen ervan) uit verschillende opties zijn opgebouwd: ze zijn hybride van aard. Dit wordt geïllustreerd in Figuur 10, waarin een keten is weergegeven waarbij voor zowel de zowel de criteria 'invloed', 'dynamiek' als 'topologie' in dezelfde ketens verschillende varianten optreden.



Figuur 10: Hybride ICT-ketens.


trust

Appendix B: Bestaande raamwerken voor trust

Voorgaand onderzoek heeft aangetoond dat voor het identificeren van normatiek er een onderscheid dient te worden gemaakt voor de verschillende type relaties, b.v. interpersoonlijk, persoon-naar-bedrijf, en interorgnanisatorisch. In dit referaat ligt de nadruk op de inter-organisatorische vertrouwensrelatie (bedrijf-naar-bedrijf).

Uit de bestaande literatuur blijkt dat er (ondanks aanzienlijke academische interesse) nog veel verschillende insteken bestaan en dat de theorie hierover nog steeds in ontwikkeling is. Verschillende studies nemen verschillende aanpakken, afhankelijk van de achtergrond van de onderzoekers en de context waarin het onderwerp van vertrouwen wordt onderzocht.

In deze appendix zijn ter illustratie een tweetal raamwerken uit bestaande literatuur opgenomen die voor de diverse type relaties weergegeven wat de elementen zijn die de mate van vertrouwen bepalen. Het betreft een raamwerk voor vertrouwen bij interpersoonlijke relaties (paragraaf B.1) en een raamwerk voor vertrouwen bij inter-organisatorische relaties (paragraaf B.2).

Derhalve zijn voorbeelden zoals opgenomen in deze appendix ook voornamelijk illustratief van aard, zonder daarbij een claim op het 'ultieme en volledige' model te zijn.

B.1 Vertrouwen bij interpersoonlijke relaties

Tabel 7 geeft een overzicht van de aspecten die interpersoonlijk vertrouwen bepalen (persoon – naar – persoon, P2P). Dit overzicht is een samenvatting van het boek [COVEY] over dit onderwerp, en is een copy van de uitwerking hiervan zoals opgesteld door de docent J. Otten, docent in het vak 'Praktijkcasussen en Vaardigheden', zoals gegeven in het 2e studiejaar van de ITA opleiding aan de EUR (2011/2012).

P2P.1: Recht op de man af spreken		P2P.2: Handelen met respect
Gedragskenmerken: • is oprecht • spreekt de waarheid • maakt duidelijk waar hij voor staat • drukt zich helder uit • noemt de dingen bij de naam; draait niet om dingen heen • manipuleert niet, verdraait de feiten niet • verdraait de waarheid niet • wekt geen valse indruk		Gedragskenmerken: • geeft echt om anderen • toont betrokkenheid • respecteert personen en de functies die zij bekleden • behandelt mensen met respect • doet niet alsof

P2P.3: Transparant zijn		P2P.4: Fouten herstellen
Gedragskenmerken: • vertelt de dingen zo dat ze te controleren zijn • is realistisch en oprecht • is open en authentiek • betracht openheid (letterlijk: heeft soms de neiging te open te zijn) • doet zich niet anders voor dan hij is • heeft geen verborgen agenda • houdt geen informatie achter		Gedragskenmerken: • maakt goed / herstelt wat fout is gegaan • aarzelt niet zijn excuses aan te bieden • herstelt / compenseert waar mogelijk • verbergt niets / houdt niets achter • is bereid het juiste te doen ook als hij daarvoor zijn persoonlijke trots opzij moet zetten
P2P.5: Loyaal zijn		**P2P.6: Resultaat laten zien**
Gedragskenmerken: • spreekt over derden op een manier alsof zij persoonlijk aanwezig zijn • vertegenwoordigt anderen die niet voor zichzelf kunnen spreken • spreekt geen kwaad achter iemands rug om • onthult geen vertrouwelijke informatie over anderen		Gedragskenmerken: • heeft eerder resultaten laten zien • krijgt de goede dingen voor elkaar • krijgt dingen voor elkaar • doet waarvoor hij is ingehuurd • realiseert tijdig en binnen afgesproken budgetten • belooft niet te veel en levert wat is afgesproken • komt niet met uitvluchten voor niet nagekomen afspraken
P2P.7: Streven naar verbetering		**P2P.8: Realistisch zijn**
Gedragskenmerken: • werkt aan verbeteringen • vergroot / verbetert competenties • blijft leren • ontwikkelt formele en informele feedbacksystemen • doet wat met gegeven feedback • voelt zich niet te goed voor feedback • is zich ervan bewust dat kennis en vaardigheden van nu wellicht onvoldoende zijn in de toekomst		Gedragskenmerken: • ziet de realiteit onder ogen en maakt zaken bespreekbaar; vat de koe bij de horens • benoemt zaken direct • neemt [in dit opzicht] het voortouw in gesprekken • weet de angel uit gesprekken te halen; kan de-escaleren • draait niet om de echt belangrijke dingen heen • stopt zijn kop niet in het zand
P2P.9: Duidelijkheid scheppen over verwachtingen		**P2P.10: Verantwoordelijkheid nemen**
Gedragskenmerken: • maakt verwachtingen duidelijk • bespreekt verwachtingen • toetst verwachtingen • onderhandelt over verwachtingen wanneer nodig en mogelijk • wekt geen valse verwachtingen • gaat er niet zomaar vanuit dat verwachtingen over en weer duidelijk c.q. wederzijds zijn		Gedragskenmerken: • voelt zich verantwoordelijk; legt rekenschap af • spreekt anderen aan op hun verantwoordelijkheid • neemt verantwoordelijkheid voor resultaten • is duidelijk over de manier waarop hij rekenschap aflegt en hoe hij anderen daarop aanspreekt • duikt niet weg voor verantwoordelijkheden; schuift verantwoordelijkheid niet af • geeft anderen niet de schuld; wijst niet naar anderen

P2P.11: Actief luisteren		P2P.12: Afspraken nakomen
Gedragskenmerken: • luistert voor hij spreekt • toont begrip • kan problemen benoemen en diagnosticeren • luistert niet alleen, maar observeert ook en kan zich inleven • heeft kennis van en inzicht in het gedrag van medewerkers en collega's • heeft niet de pretentie te weten wat anderen het belangrijkst vinden • doet niet alsof hij overal een antwoord op weet		Gedragskenmerken: • zegt wat hij doet (gaat doen) • doet wat hij heeft toegezegd • is zorgvuldig in het doen van toezeggingen en houdt zich er aan • stelt er een eer in zich aan toezeggingen te houden • schendt het vertrouwen niet • denkt niet lichtvaardig over het breken van beloften of het niet nakomen van toezeggingen
P2P.13: Vertrouwen geven		
Gedragskenmerken: • laat zien dat hij van vertrouwen wil uitgaan • geeft vertrouwen aan hen die dat vertrouwen waard zijn gebleken • geeft voorwaardelijk vertrouwen aan hen die dat nog moeten verdienen • durft meer vertrouwen te geven rekening houdende met de situatie en de kwaliteiten en competenties van		

Tabel 7: Aspecten van interpersoonlijk vertrouwen.

B.2 Vertrouwen bij inter-organisatorische relaties

Tabel 8 geeft een overzicht van de aspecten die vertrouwen tussen bedrijven bepalen (bedrijf-naar-bedrijf, B2B). Dit overzicht is afkomstig (geciteerd) van de publicaties gelieerd aan de OSSTM v3 [ISECOM] [ROSIELLE].

In veel andere publicaties (bijvoorbeeld [SYDOW]) zijn ook aspecten voor vertrouwen tussen bedrijven weergegeven. Voor een groot deel zijn deze overlappend, voor een klein deel zijn ze aanvullend aan de aspecten benoemd in Tabel 8. Omdat er hier niet gestreefd wordt naar volledigheid, zijn deze echter niet in deze appendix opgenomen.

B2B.1: Omvang van infrastructuur (Engels: Size)		B2B.2: symmetrie van vertrouwen (Engels: Symmetry of trust)
Het aantal subjects waartoe het vertrouwen zich uitstrekt. Stelt de source vertrouwen in slechts een subject of in meerdere? En moeten die subjects zelf ook weer derden vertrouwen? Hoe groter de size, hoe groter het vertrouwen moet zijn en hoe meer maatregelen er nodig zijn.		Dit gaat om de richting waarin het vertrouwen plaatsvindt. Bent u afhankelijk van een ander, de ander van u of is er een wederzijdse afhankelijkheid? Als u niet afhankelijk bent van de ander, is er geen reden voor wantrouwen. Bij wederzijdse afhankelijkheid moet de ander rekening houden met de gevolgen als het vertrouwen geschonden wordt.
B2B.3: Transparantie **(Engels: Transparency)**		**B2B.4: Control** **(Engels: Control)**
De mate van zichtbaarheid van alle operationele onderdelen en processen van het subject en zijn omgeving. De zichtbaarheid hoeft zich niet per se uit te strekken tot de source. Ook als de source weet dat het subject soms zichtbaar is voor derden, kan het vertrouwen al toenemen. De zichtbaarheid wordt beschouwd voor zover relevant voor het vertrouwen, bijvoorbeeld tijdens kantooruren of op specifieke locaties.		De mate van invloed die de source kan uitoefenen op het subject. Vaak is deze invloed beperkt in tijd, zoals bij een werkrelatie (manager/ondergeschikte) of vrijheidstraf (cipier/gevangene). Tijdens een audit wordt alleen de werkelijk uitgeoefende invloed in beschouwing genomen. De mogelijkheid om het subject te beïnvloeden op zichzelf telt niet mee.
B2B.5: Consistentie **(Engels: Consistency)**		**B2B.6: Integriteit** **(Engels: Integrity)**
Dit is historisch bewijs van compromitteren of corruptie van het subject. Wat het subject in het verleden gedaan heeft, kan een indicatie zijn voor toekomstig gedrag. Hoe vaak heeft het subject al eerder vertrouwen geschonden? Kijk hierbij niet alleen naar het aantal feiten waaruit onbetrouwbaarheid blijkt, maar tel ook de feiten die op betrouwbaarheid wijzen. Let ook niet alleen op absolute aantallen, maar neem ook de frequentie mee in de beschouwing. Neemt het gedrag toe of af? Of is er een samenhang met bepaalde andere gebeurtenissen?		De mate waarin het gedrag van het subject verandert in de loop der tijd. Alles en iedereen verandert in de loop der tijd. Let op aanwijzingen waaruit de veranderingen in gedrag van het subject blijken. Die aanwijzingen kunnen ook indirect zijn. Als derden die aanwijzingen verstrekken, weet dan wel in welke mate die derde te vertrouwen is.
B2B.7: Compensaties **(Engels: Offsets)**		**B2B.8: Waarde van compliance** **(Engels: Value of reward)**
Compensatie moet voldoende waarborg geven voor financiële vergoeding aan de source of boete aan het subject als het vertrouwen geschonden wordt.		De financiële winst of opbrengst voor de source is voldoende hoog om het risico van de trust te compenseren. Het gaat hier vooral om persoonlijk gewin en niet om een dwangmiddel zoals bij compensatie.

B2B.9: Componenten (Engels: Components)		B2B.10: Kwetsbaarheid (Engels: Porosity)
Dit is het aantal elementen dat voorzieningen aan het subject levert en waarvan het subject afhankelijk is. Zelfs als een computer volkomen betrouwbaar is, hoeft dat niet te gelden voor de data, de stroomvoorziening, de gebruikersinvoer, etc.		De mate van veiligheid waarin het subject verkeert. Het geeft de balans weer tussen het geheel van contact met/toegang tot het subject, beveiligingsmaatregelen en beperkingen.

Tabel 8: Aspecten van vertrouwen tussen bedrijven.


trust

Appendix C: Concept artikel *'C⁴-model'*

Deze appendix bevat een concept van het artikel '*Een model voor de beheersing en controle van ICT-ketens - Het Chain Content, Context & Control (C⁴-) model*'.

De definitieve versie van dit artikel zal in het derde kwartaal van 2012 ter publicatie worden aangeboden, met als optie het Norea tijdschrift 'de IT-Auditor'.

Een model voor de beheersing en controle van ICT-ketens

Het Chain Content, Context & Control (C4-) model

Het belang van ICT-ketens neemt sterk toe en daarmee ook het belang van beheersing daarvan. Bestaande modellen voor beheersing en controle van ICT zijn echter veelal intra-organisatorisch gericht, en niet op ICT-ketens. Dit artikel beschrijft het C⁴-model voor de beheersing en controle van ICT-ketens. Dit model geeft de gebruiker een hulpmiddel voor het identificeren en afbakenen van het te beheersen onderwerp. Voor de controle geeft het model handvatten om de kwaliteitsbeheersing van een ICT-keten te beoordelen. Het model helpt daarmee bij zowel het identificeren van de hiaten in de kwaliteitsbeheersing van ICT-ketens als bij het uitvoeren van audits hierop.

Harrie Bastiaansen, Ype van Wijk

1. Inleiding

In de maatschappij neemt het belang van ICT-ketens sterk toe. Bij ICT-ketens gaan ICT-diensten en -infrastructuren over de grenzen van bedrijven en bedrijfsonderdelen heen. Niet alleen neemt het aantal ICT-ketens sterk toe, ook worden ze steeds complexer: ze ondersteunen meer functionaliteit en er zijn steeds meer partijen (ketenpartners) betrokken.

Met het toenemend belang van ICT-ketens neemt ook het belang toe van de kwaliteitsbeheersing en de controle daarvan. Met het groeiend belang van ICT-ketens en de 'robuustheid' daarvan neemt ook het belang van de beheersing van ICT-ketens en ICT-ketenaudits toe. Getuige hiervan zijn de Norea werkgroep voor ketenauditing [NOREA], onderzoeksinitiatieven bijvoorbeeld in de EU [ENISA] en Nederland [SEQUAL] en voorgaande publicaties in het Norea tijdschrift 'de IT-auditor' over ICT-ketenauditing [EDPAUDITOR1] – [EDPAUDITOR4].

Het Nederlands onderzoeksproject TTISC [TTISC] werkt momenteel aan een assurance raamwerk voor ICT-keten beheersing en controle. Als resultaat daarvan presenteren we in dit artikel Chain Content, Context & Control model (het C⁴-model). Dit model bestaat uit drie delen:

(1) de *content*, gericht op wat het te beheersen onderwerp in de ICT-keten inhoudt,

(2) de *context*, gericht op het perspectief van waaruit beheersing of beoordeling van de in ICT-ketens plaatsvindt en

(3) de *control*, gericht op de vraagstelling hoe controle op beheersing in ICT-ketens kan worden vormgegeven.

In dit artikel ligt de nadruk op het model voor ICT-ketenbeheersing. In een vervolgartikel zullen we specifiek de control-component voor de beheersing van ICT-ketens verder uitdiepen.

De volgende paragraaf belicht de doelstelling van een integraal model voor de beheersing van ICT-ketens toegelicht, gevolgd door de opzet voor zo'n model. De paragrafen 4-6 gaan achtereenvolgens in op de individuele componenten van

het model: de content, context en control. De afsluitende paragraaf 7 vat de resultaten hiervan samen samengevat in een detaillering van het integrale C^4-model, aangevuld met conclusies en aanbevelingen.

2. Doelstelling voor een integraal model voor ICT-ketenbeheersing

Zoals in de inleiding aangegeven, staat het onderwerp van beheersing en controle van ICT-ketens volop in de belangstelling. Het onderwerp kan daarbij vanuit een groot aantal verschillende oogpunten bekeken worden, hetgeen eenduidige communicatie hierover lastig maakt. Ergo, uit de praktijk is de behoefte ontstaan naar een gedegen model om de diverse perspectieven op ICT-ketenbeheersing te kunnen positioneren, relateren en bespreken, zoals ook benoemd in de literatuur (citaat [RAVAL], bladzijde 49/50):

For a complete and comprehensive solution to its control needs, a business needs a systemic framework for control system development. Without an overarching model (a framework), it would be almost impossible to prove risks are managed well and as completely as necessary. Frameworks permit us to define the scope of control and security systems within a business.

Voor de intra-organisatorische beheersing van ICT bestaat al een veelheid aan modellen en auditraamwerken. Modellen voor ICT-beheersing, auditing en assurance raamwerken, governance richtlijnen en nog vele andere (al dan niet technische richtlijnen) zijn eerder opgesteld vanuit o.a. de internationale accountants praktijk (IFAC), de IT audit professie (ISACA), de ISO standaardisatie omgeving. Echter, nagenoeg alle modellen en richtlijnen zijn opgesteld vanuit intra-organisatorisch perspectief.

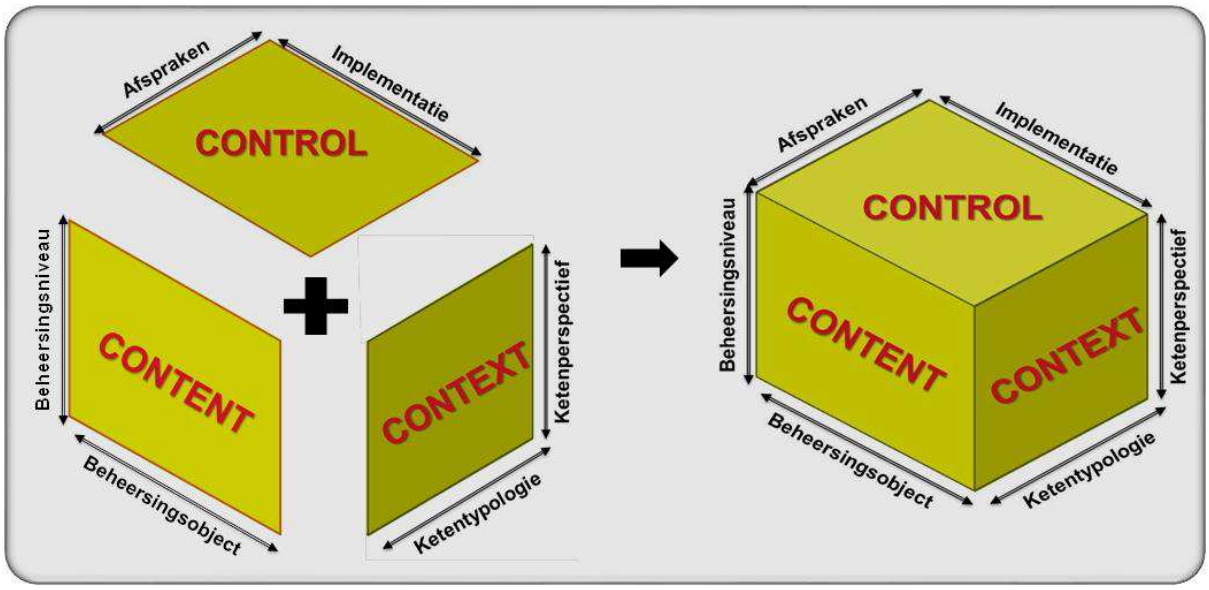
Momenteel ontbreken nog de overeenkomende modellen en richtlijnen voor automatisering in ICT-ketens. Een aantal aspecten maakt de beheersing van ICT-keten anders. In ICT-ketens is sterke governance niet een ‘gegeven’. Er is geen (strikte) ‘line of command’. De span of control voor individuele organisaties is beperkt. Vaak moeten beslissingen middels consensus worden genomen. Daarnaast zijn kosten, baten en doelstellingen niet eenduidig voor alle ketenpartners en ze zijn ook niet noodzakelijkerwijs evenredig verdeeld over alle ketenpartners. Tot slot kunnen er communicatie- en cultuurverschillen zijn tussen ketenpartners. Zelfs binnen hetzelfde land kunnen verschillende sectoren specifieke terminologie hanteren. Een gedeeld begrip en afstemming in de communicatie zijn van groot belang.

Om aan de behoefte aan een integraal model voor ICT-ketenbeheersing te voldoen heeft het onderzoeksproject TTISC het initiatief genomen om zo’n integraal model op te stellen, daarbij zoveel mogelijk hergebruik makend van bestaande modellen. Dit model wordt in het vervolg van dit artikel verder beschreven.

3. De opzet van het integraal model voor ICT-ketenbeheersing

Een basiseis aan een integraal model voor ICT-ketenbeheersing is dat het zowel de verschillende onderwerpen van ICT-ketenbeheersing (ofwel de ‘content’) benoemt, de verschillende perspectieven beschouwt van waaruit beheersing en beoordeling van ICT-ketens plaatsvindt (ofwel de ‘context’) als de methoden omvat waarop control kan worden uitgeoefend (ofwel de ‘control’).

Het C^4-model omvat deze onderwerpen content, context en control. Het model splitst elke van de onderwerpen verder uit in twee assen, waardoor voor elk onderwerp een vlak ontstaat, i.e. het ‘content-vlak’, het ‘context-vlak’ en het ‘control-vlak’. Het content-vlak wordt opgespannen door de as ‘beheersingsniveau’ en de as ‘beheersingsobject’, het context-vlak door de as ‘ketentypologie’ en de as ‘ketenperspectief’, en het control-vlak door de as ‘afspraken’ en de as ‘implementatie’. Gecombineerd leiden de vlakken tot het integrale (kubusvormige) C^4-model -model voor ICT-ketenbeheersing, zoals weergegeven in Figuur 2.



Figuur 11: Het integraal C^{4-}-model voor ICT-ketenbeheersing, opgebouwd uit het 'content'-, 'context'- en 'control'-vlak.

Bij het model wordt opgemerkt dat het combineren van de drie vlakken tot een kubus louter is bedoeld ter illustratie. Het combineren van drie 2-dimensionale vlakken in één enkele 3-dimensionale kubus zonder verlies aan informatie is uiteraard niet mogelijk. Bij het gebruik van de kubus (voor bijvoorbeeld het positioneren van ICT-audits) moet daarom worden teruggegrepen op de onafhankelijke vlakken, i.e. het content-vlak het context-vlak en het control-vlak.

In de volgende paragrafen wordt elk van de vlakken met hun assen verder toegelicht, uitmondend in een detaillering van het integrale C^4-model.

4. Het content-vlak van het C4-model

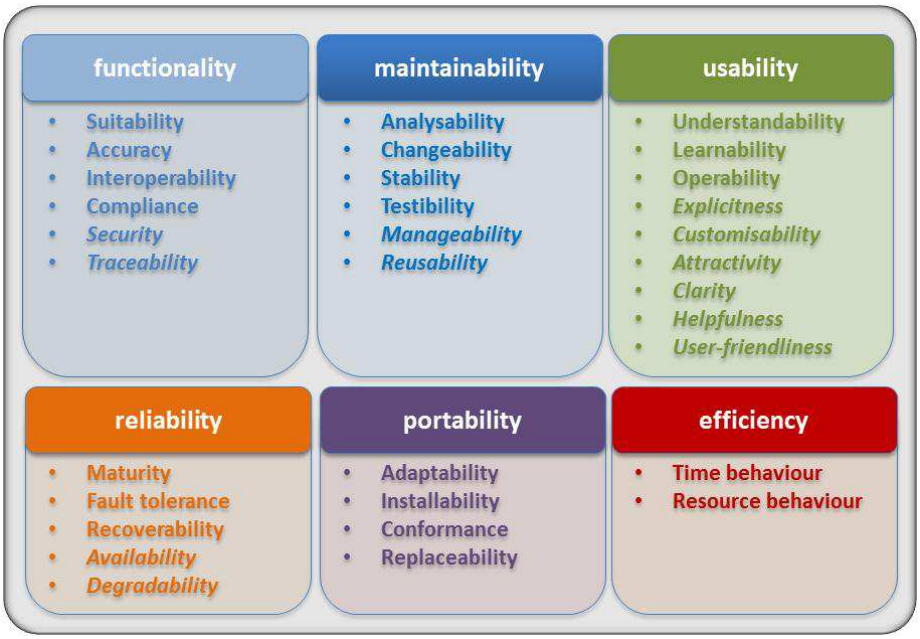
Het content-vlak wordt opgespannen door de assen 'beheersingsobject' en 'beheersingsniveau'.

De as 'Beheersingsobject'

Deze as geeft aan of het object van beheersing de (financiële) waarde van de ICT-keten betreft, de functionele onderdelen (de te leveren 'service') per ketenpartner, of de kwaliteit waarmee deze diensten en dienstonderdelen aan elkaar worden geleverd.

- *Waarde:* De strategische doelstellingen, waarde, baten en kosten van het werken en afstemmen van ketens in zijn geheel.
- *Functioneel:* Afstemming van service componenten, baten en kosten naar individuele ketenpartners.
- *Kwalitatief:* De mate waarin aan de (kwalitatieve) verplichtingen van de serviceverlening wordt voldaan.

De term kwaliteit is hierbij een breed begrip. Het kan een breed palet aan kwaliteitseigenschappen voor software systemen aanduiden, zoals bijvoorbeeld uitgewerkt in het Quint-model [QUINT] (afgeleid van de ISO/IEC norm 9126-1 [ISO]) en weergegeven in Figuur 12.



Figuur 12: Kwaliteitsaspecten volgens het Quint-model.

De as 'Beheersingsniveau'

Deze as geeft het bestuurlijke niveau aan waarop de beheersing van toepassing is. Drie beheersingsniveaus worden onderscheiden, zoals bekend uit het KAD+ model [KAD+] gericht op de beheersing van intra-organisatorische administratieve dienstverlening. Deze drie niveaus zijn:

- *Strategische beheersing:* De strategische uitgangspunten en aansturing voor de ICT-keten.
- *Organisatorische beheersing:* De vertaling van de strategische uitgangspunten naar het organisa-torische beheerskader van de ICT-keten.
- *Operationele beheersing:* De inrichting en de beheersing van de werkprocessen.

5. Het context-vlak van het model

Het context-vlak wordt opgespannen door de assen 'ketentypologie' en 'ketenperspectief'.

De as 'Ketentypologie'

De typologie geeft de wijze weer waarop de samenwerkings- en afstemmingsrelaties in een ICT-keten zijn ingevuld. Conform [GRIJPINK] vormt het basisonderscheid de mate waarin er een overkoepelend gezag in de keten is dat eisen aan ketenpartners kan opleggen over de wijze van invulling van ICT-voorzieningen. We onderscheiden drie typen:

- *Ketenkoppeling:* Bij ketenkoppeling werken ketenpartners met elkaar samen op basis afspraken over hun koppelvlak, zonder daarbij afstemming te hebben over de geleverde functionaliteit of de (kwaliteit van) de technische implementatie. Deze situatie treedt bijvoorbeeld op wanneer diensten op dynamische wijze middels service oriëntatie worden afgenomen.

- *Ketenafstemming:* Bij ketenafstemming stemmen ketenpartners wel de functionaliteit en de kwaliteit op elkaar af. Op basis van consensus kunnen daarbij beslissingen worden genomen. Een voorbeeld hiervan is de situatie waarin ketenpartners op basis van gedeeld belang met elkaar de kwaliteit van hun technische implementatie bespreken, risico's en zwakheden identificeren en eventueel tot (technische of procesmatige) compenserende maatregelen besluiten zoals bijvoorbeeld in [BASTIAANSEN2] beschreven voor het kwaliteitsaspect continuïteitsmanagement. Als speciale uitingsvormen hiervan kunnen het afgeven van een Service Level Agreement (SLA) of een Third Party Mededeling (TPM) worden genoemd.

- *Ketensturing:* Bij ketensturing is er sprake van een ketenpartner met voldoende overkoepelend gezag om eisen aan ketenpartners op te kunnen leggen over de wijze van invulling van hun ICT-voorzieningen. Dit zowel bijvoorbeeld doordat er een ketenpartner is met een dominante marktpositie of doordat er vanuit wet en regelgeving eisen worden opgelegd.

In zijn algemeenheid zullen ICT-ketens hybride van aard zijn: één van bovenstaande types zal niet voor alle relaties in de keten van toepassing zijn.

De as 'Ketenperspectief'

Het ketenperspectief beschrijft de optiek van waaruit de ICT-keten wordt beschouwd. De volgende perspectieven worden daarbij onderscheiden:

- *Het toezichtperspectief:* In dit perspectief wordt de gehele ICT-keten van 'buitenaf' beschouwd ten einde over de compliance aan wet- en regelgeving te kunnen oordelen.

- *Het ketenperspectief:* In dit perspectief wordt de gehele ICT-keten (als het ware van 'buitenaf') beschouwd ten einde te kunnen oordelen over een beheersingsaspect van de ICT-keten in zijn geheel, bijvoorbeeld de eind-tot-eind beheersing (i.e. organisatorisch en operationeel) van business continuïteit.

- *Het partnerperspectief:* In dit perspectief wordt een aspect beschouwd vanuit een specifieke partij (en ketenpartner) binnen de ICT-keten. Niet de gehele ICT-keten wordt beschouwd maar het belang van slechts één enkele schakel hierin.

6. Het control-vlak van het model

Het control-vlak wordt opgespannen door de assen 'afspraken' en 'implementatie'.

De as 'Afspraken'

De afspraken omvatten de (contractuele) afspraken tussen de ketenpartners, zoals vastgelegd in een Service Level Agreement (SLA). De volgende aspecten zijn van belang bij control en beoordeling van de gemaakte afspraken:

- *Volledigheid:* Zowel de (technische) kwaliteitsaspecten als de procesinteracties dienen in de afspraken met voldoende diepgang en detail te zijn benoemd. Als voorbeeld van de eerstgenoemde kan het kwaliteitsaspect 'beschikbaarheid' worden genoemd, uitgedrukt in bijvoorbeeld zowel minimaal percentage beschikbaarheid, maximaal aantal incidenten per jaar en maximale duur van de verstoring per incident. Als voorbeeld van laatstgenoemde kunnen procesafspraken rondom (business continuïteit) worden genoemd [BASTIAANSEN1].

- *Betrouwbaarheid:* De betrouwbaarheid van afspraken dienen een waarheidsgetrouwe afspiegeling te geven van de implementatie en getroffen maatregelen door de aanbieder. Hier komt het aspect 'vertrouwen' om de hoek kijken, met het instrument 'trust audit' [BASTIAANSEN2] ter beoordeling hiervan.

- *Aaneenschakeling:* Dit omvat de aaneenschakeling van de afspraken die tussen de diverse ketenpartners op de verschillende plaatsen in de ICT-keten zijn afgesproken. Zijn ze consistent? Hoe 'tellen' de verschillende afspraken bij elkaar op tot het vereiste niveau van beheersing van de gehele keten. Het is mogelijk hiervoor wiskundige modellen te ontwikkelen die uitwerking van de concatenatie van afspraken op de beheersing en kwaliteit van de gehele keten bepalen [SEQUAL], waar zelfs de betrouwbaarheid van gemaakte afspraken in kan worden verdisconteerd [TTISC].

De as 'Implementatie'

De implementatie omvat de daadwerkelijke bestuurlijke en technische maatregelen die in de ICT-keten en door ketenpartners zijn genomen om beheersing van de ICT-ketens te realiseren, bijvoorbeeld de maatregelen om het kwaliteitsaspect 'beschikbaarheid' te verhogen. Zoals vertrouwd zal voorkomen in de audit professie, zijn de volgende aanpakken daarbij te onderscheiden:

- *Systeemgericht:* Dit betreft de besturings- en beheersings-processen en maatregelen. Deze dienen op zodanige wijze te zijn vormgegeven zodat de beheersing van de keten adequaat is.

- *Gegevensgericht:* De (uitwisseling van) gegevens in de ICT-keten is hetgeen waar het uiteindelijk om gaat. Dit betreft derhalve het inrichten van de keten waardoor het niveau van control zodanig is ingericht dat de inhoud i.e. de (kwaliteit van de gegevens) binnen de waardeketen juist en controleerbaar is.

- *Distributiegericht:* De distributiegerichte controle aanpak is gericht op de beoordeling van de implementatie van de ICT-ketens middels applicaties en infrastructuur (zowel servers als operating systemen) om van voldoende beheersing van de ICT-keten te kunnen spreken. Hieronder vallen implementatiegerichte maatregelen zoals redundantie (om beschikbaarheid te verhogen), encryptie (om vertrouwelijkheid te verhogen) en informatievalidatie (om integriteit te borgen).

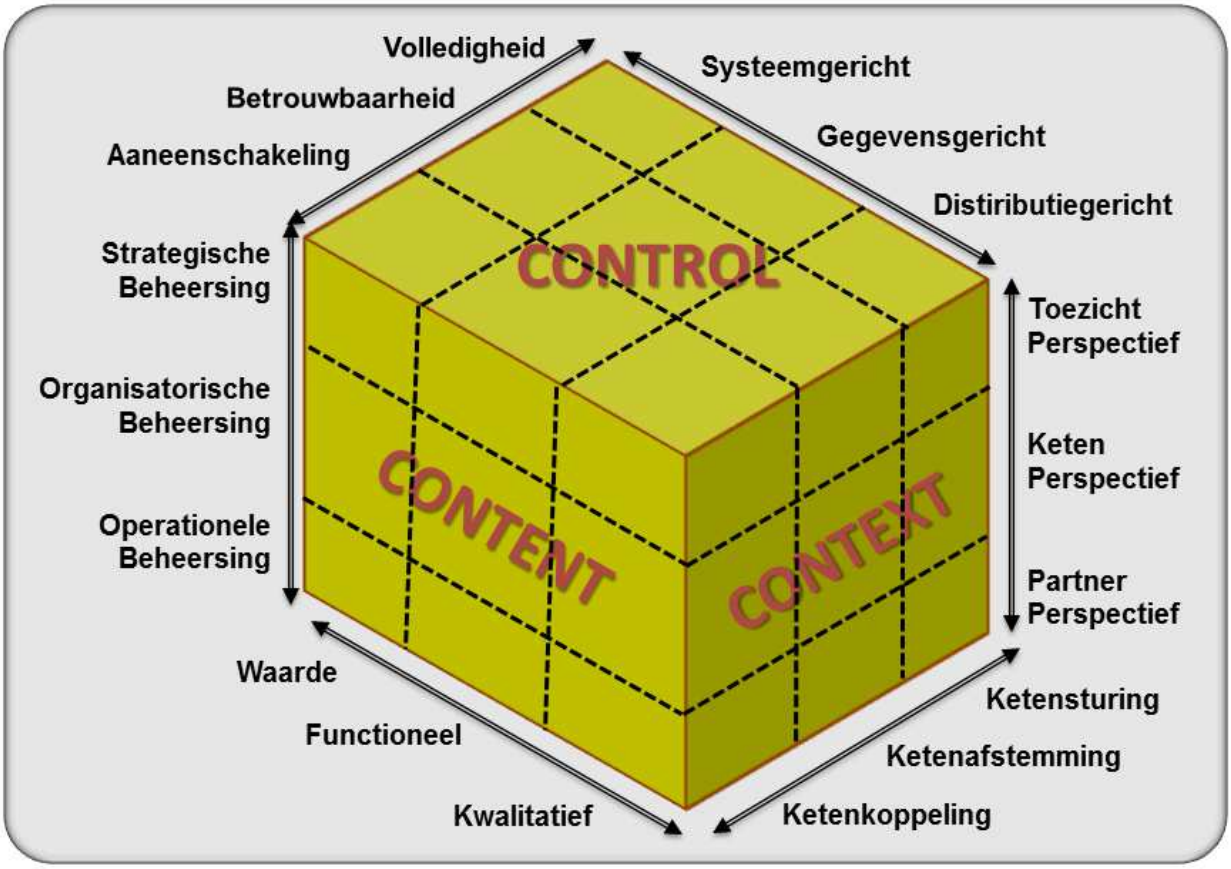
Een vervolgartikel zal gaan over Assurance en Governance in ketens. Hierbij komen de specifieke assurance-determinanten voor de beheersing van ICT-ketens aan de orde. De kwalitatieve determinanten voor assurance in ketens zijn gebaseerd op risico-control componenten en worden in een service business context geplaatst.

7. Tot slot

In dit artikel hebben we een model voorgesteld en uitgewerkt voor de beheersing en controle van ICT-ketens. Het geeft een handvat om het totale speelveld van ICT-ketenbeheersing te overzien, hiaten hierin te identificeren en communicatie hierover te vergemakkelijken. Daarbij kan het model tevens dienen om de scope van ICT-ketenaudits te bepalen.

De sterkte van model is dat het vanuit zowel een content, context als control perspectief is vormgegeven, waardoor het de grote diversiteit aan en wijze van kijken naar ICT-ketens afdekt. Daarmee is het model een goed hulpmiddel in het beheersen en auditen van ICT-ketens.

Met de uitwerking van de content-, context- en control-vlakken op beide assen uit de voorgaande paragrafen, ontstaat de gedetailleerde uitwerking van het integraal C^4-model voor ICT-ketenbeheersing zoals weergegeven in Figuur 3.



Figuur 13: Uitwerking van het integraal C^4-model voor ICT-ketenbeheersing.

We merken op dat volledige beheersing van ICT-ketens niet vereist dat beheersing op elk van de snijpunten uit de kubus van het C^4-model plaatsvindt. Zoals eerder is aangegeven, dient de samenvoeging van de individuele vlakken tot een kubus alleen illustratieve doeleinden. Veel meer ligt de meerwaarde om voor specifieke ICT-ketens per vlak de afweging te maken welke van de aspecten voor beheersing en controle als relevant wordt beoordeeld.

Wij roepen hierbij organisaties tevens op om deze tezamen met ons dit model voor het beheersen van ICT-ketens en het positioneren van ketenaudits voor hun (bedrijfs-) of ketensituatie verder te beproeven en ontwikkelen. Het verder moduleren van het model door de ontwikkeling van best practices en governance richtlijnen voor ketens zou hierbij een goede vervolgstap kunnen zijn.