Het construeren van **referentiekaders**: een principle-based aanpak

Het beoordelen van auditobjecten wordt uitgevoerd op basis van een mix van normen, samengebracht in een zogeheten referentiekader. Voor het uitvoeren van consistente evaluaties vervult een referentiekader dan ook een belangrijke rol. In de huidige praktijk wordt de samenstelling van referentiekaders niet ondersteund door een wetenschappelijk onderbouwde methodiek. In dit artikel wordt een werkwijze gepresenteerd waarmee auditors een referentiekader op een systematische wijze kunnen ontwikkelen of evalueren. Dit artikel is gebaseerd op een in 2010 bij de VU afgerond promotieonderzoek van de eerste auteur [TEWA10].

WIEKRAM TEWARIE, RONALD PAANS EN JORIS HULSTIJN

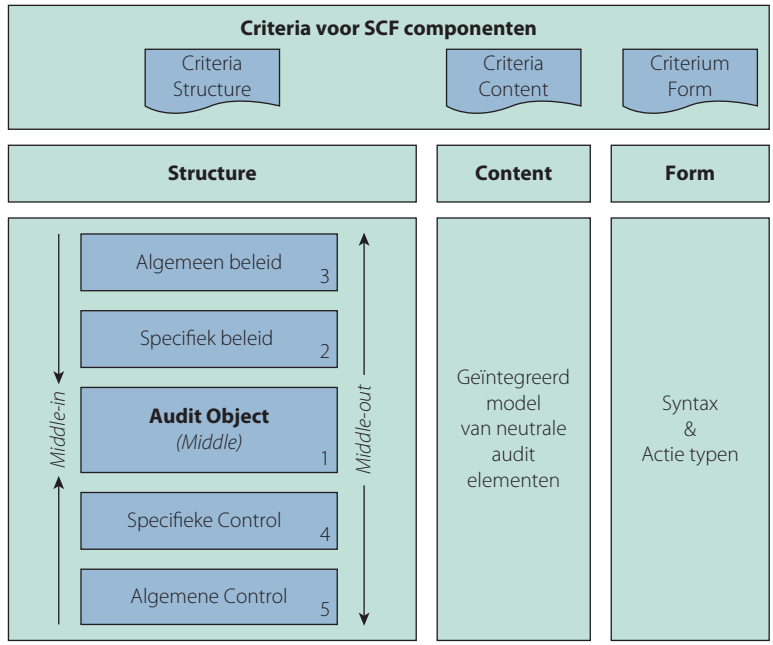
Bij het ontwikkelen van een referentiekader wordt een auditor geconfronteerd met een variëteit aan omgevingsaspecten, zoals conditionele, resources- en managementaspecten. De auditor ontwikkelt het referentiekader doorgaans op basis van de eigen ervaring, kennis, kunde en de beschikbare best practices, zoals: Cobit, NIST, Standard of Good Practice, ITIL en ASL. Het ontwikkelen van een referentiekader betekent dat de auditor een set auditcriteria selecteert uit de best practices en aanpast aan de specifieke situatie. Vaak moeten auditors criteria zelf formuleren. Een referentiekader bevat in de regel dan ook een mix van generieke en gedetailleerde normen. Door gebrek aan een methode voor het selecteren van de auditcriteria kan de auditor niet goed onderbouwen of de set normen voor de betreffende audit de juiste normen bevat. Er bestaat dus onzekerheid over de selectie van de juiste normen, en over de volledigheid en samenhang van het referentiekader. In feite wordt hiermee dus een auditrisico gelopen.

Het gebrek aan een methode voor het samenstellen van referentiekaders heeft ons ertoe bewogen om een methodisch raamwerk te ontwikkelen, gebaseerd op wetenschappelijke gronden, waarmee het creëren van een samenhangend referentiekader kan worden ondersteund. Het raamwerk zou een fundamenteel instrument voor het vakgebied kunnen worden.

CONTEXT VERBETERDE AANPAK

Het conceptueel raamwerk waarmee de gewenste verbetering kan worden bereikt, gaat uit van een zogeheten *principle based* aanpak. We gaan uit van principes omdat die in beperkte mate onderhevig zijn aan verandering, veroudering of aan technologische ontwikkelingen.

Het conceptueel raamwerk bestaat uit drie componenten, *Structure*, *Content* en *Form* (SCF). De relatie tussen deze drie componenten wordt geschetst in figuur 1. De component Structure verdeelt het auditdomein in een aantal horizontale lagen. Het auditobject wordt in context geplaatst met twee conditionele lagen en twee controllagen. Zo staat het auditobject altijd centraal. De component Content refereert aan de identificatie van auditelementen per onderkende laag. De component Form refereert aan een syntax, een voorschrift voor het vastleggen van auditprincipes. Deze SCF-componenten voldoen aan een aantal vooraf gedefinieerde criteria. Naast deze drie componenten bevat het conceptueel raamwerk ook een toepassingscomponent die in drie stappen beschrijft op welke wijze de auditelementen geselecteerd kunnen worden. De stappen zijn *Middle*, *Middle-out*, *Middle-in* (M3). Deze ▸



Figuur 1: Overzicht van de relatie tussen de onderkende lagen en drie ontwikkelstappen (M3: middle, middle-out, middle-in) en de relatie tussen de componenten Structure, Content en Form (SCF). Elk component voldoet aan vooraf vastgestelde criteria.

SCF-componenten worden verder in dit artikel behandeld en verduidelijkt met behulp van voorbeelden.

CRITERIA VOOR DE SCF-COMPONENTEN

Volgens de IFAC ISAE 2000 (2003) standaard dient een referentiekader aan vijf kwaliteitscriteria te voldoen: relevantie, volledigheid, betrouwbaarheid, neutraliteit en begrijpelijkheid. Wij hebben naast deze criteria additionele criteria geïdentificeerd uit andere bronnen, zoals *software requirements* [BOEH78]. Tabel 1 geeft een overzicht van de criteria in relatie tot het SCF-raamwerk.

Structure

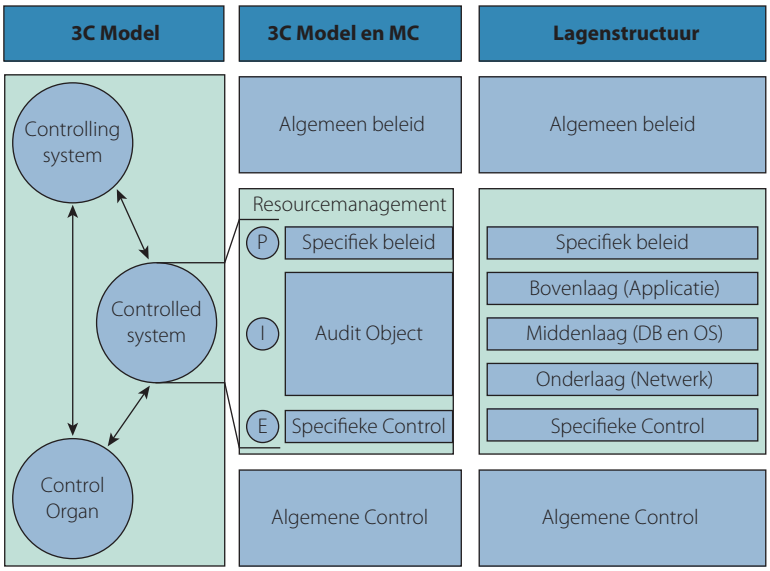
Om tot een samenhangende splitsing van het auditdomein te komen en hiermee de structuur van het referentiekader te ontwikkelen hebben we een functionele benadering uit de systeemtheorie toegepast, ook wel de 'black box-benadering' genoemd. Hierbij wordt de nadruk gelegd op externe relaties tussen systemen. Hiervoor hebben we gebruikgemaakt van het 3C-model (*Controlling system, Controlled system en Control organ*) [LEEU74], [BUNG79][1] en de managementcyclus (MC) *Planning, Implementation* en *Evaluation* [STAR02], twee cyclische modellen. Door de combinatie van deze twee modellen ontstaat een gelaagde structuur die voldoet aan de criteria voor het SCF-raamwerk en systeem(gedrags)eigenschappen.
Zoals in figuur 2 is geïllustreerd kan de auditomgeving op basis van de 3C en MC-modellen worden onderverdeeld in een lagenstructuur. Deze lagenstructuur is nodig om een compleet overall beeld van het auditobject, inclusief de afhankelijkheden binnen deze omgeving, te verkrijgen.

IFAC-ISAE 2000 en additionele criteria	
Structure	Gestructureerdheid en coherentie
Content	Betrouwbaarheid, volledigheid, relevantie, neutraliteit, begrijpelijkheid, transparantie, herbruikbaarheid, geïntegreerdheid en coherentie
Form	Consistentie

Tabel 1: Overzicht van IFAC (2003) en additionele referentiekader criteria

Een auditomgeving omvat een veelheid van aspecten, zoals conditionele aspecten, inrichtingsaspecten en managementaspecten. De auditor zal deze mix van aspecten in de juiste context en op het juiste niveau moeten positioneren. Het doel van de toepassing van het 3C-model is om door middel van de onderkende gebieden een splitsing van deze mix van auditaspecten af te dwingen en tegelijkertijd deze aspecten in een juiste contextuele samenhang te positioneren. Vanuit deze context kunnen ook de risico's worden geïdentificeerd. De betekenissen die aan de uiteindelijke lagen worden toegekend zijn:

- Algemeen beleid. Vertegenwoordigt in de praktijk een domein van waaruit invloed op de overige twee domeinen, auditobject en algemene control, wordt uitgeoefend. Algemeen beleid bevat conditionele aspecten en randvoorwaarden, zoals hoofdbeleid, strategie, regelgeving en uitgangspunten voor business- en IT-architectuur.
- Specifiek beleid. Vertegenwoordigt in de praktijk een domein dat specifieke conditionele aspecten bevat die van toepassing zijn op het auditobject. Deze specifieke conditionele aspecten zijn gerelateerd aan algemene beleidsaspecten.
- Bovenlaag. Is een gebruikers-, proces- en applicatie georiënteerd domein. Het bevat onder andere proces- en applicatie-aspecten van het auditobject.
- Middenlaag. Vertegenwoordigt de verwerkingslaag (databases en platform) van het auditobject en vervult de rol van mediator of integrator.
- Onderlaag. Vertegenwoordigt de communicatielaag van het auditobject.
- Specifieke control. Vertegenwoordigt een domein dat specifieke



Figuur 2: De correspondentie tussen de subsystemen en lagenstructuur

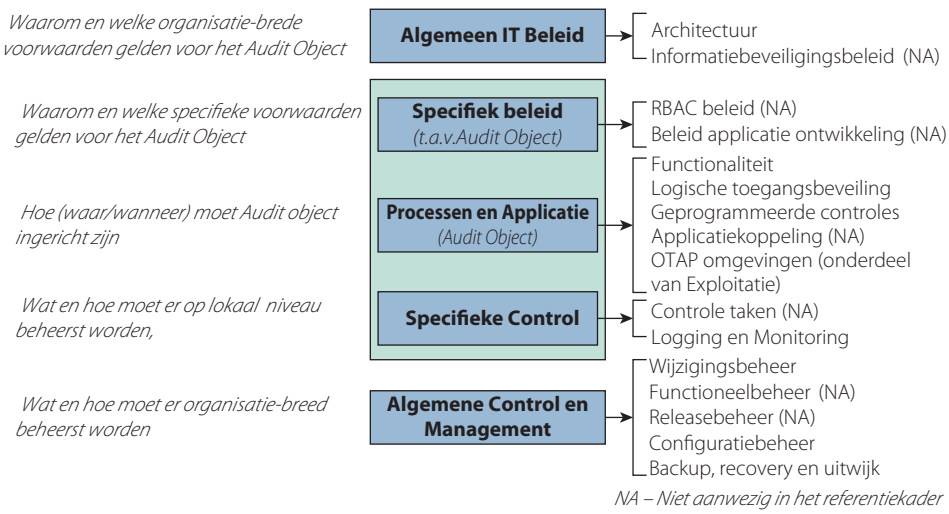
control- en evaluatie-aspecten ten aanzien van het auditobject bevat. Er wordt nagegaan in hoeverre er bij de inrichting van het auditobject, zoals de processen en IT-objecten, controlinstrumenten zijn ingebouwd om de inrichting van de processen en IT-objecten te beheersen. Dit is kortcyclisch van aard.

- Algemene Control. Vertegenwoordigt een waarnemings- en beheersingsinstrument. Het is een omgeving van waaruit het auditobject wordt gemanaged en vervult hiermee een controlfunctie die langcyclisch van aard is. Binnen dit domein worden de noodzakelijke beheersprocessen voor het Audit Object vastgesteld en wordt nagegaan hoe deze processen zijn vormgegeven om de inrichting van het betreffende auditobject continue in control te houden, zoals IT-service-support en managementprocessen.

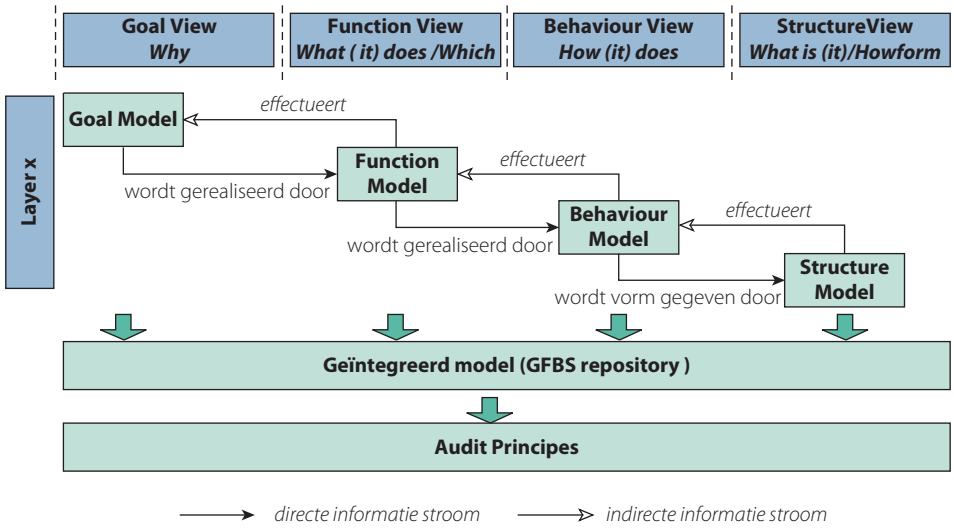
Voorbeeld: Een auditor ontwikkelt in de praktijk een referentiekader voor een applicatie als auditobject. Gegeven is dat de applicatie enkele jaren oud is, dat er voordurend functionele wijzigingen plaatsvinden en dat het technisch beheer van de applicatie, het beheer van de database, het platform en de netwerkinfrastructuur zijn uitbesteed. Het referentiekader is opgebouwd op basis van de volgende onderwerpen: Exploitatiebeheer, Wijzigingsbeheer, Configuratiebeheer, Logische toegangsbeveiliging, Logging en monitoring, Back-up, recovery en uitwijk, Geprogrammeerde controlemaatregelen, Architectuur en Functionaliteit. De vraag is of dit referentiekader gestructureerd is en of alle relevante onderwerpen zijn meegenomen. In figuur 3 worden deze onderwerpen geprojecteerd op de ontwikkelde lagenstructuur, waarmee zichtbaar wordt gemaakt welke onderwerpen (als voorbeeld) op welke laag ook meegenomen hadden kunnen worden.

Content

De invulling van de lagenstructuur wordt gegeven door de component Content. Intuïtief kunnen diverse auditelementen per laag worden benoemd. Om willekeur aan te benoemen auditelementen te voorkomen, is het GFBS-framework (*Goal, Function, Behaviour en Structure*)[2] ontwikkeld en toegepast, zoals aangegeven in figuur 4. Dit framework is gebaseerd op de compositionele benadering uit de systeemtheorie, die zich richt op het identificeren van interne componenten en hun interne relaties binnen een systeem en wordt ook wel de 'white box-benadering' genoemd. De combinatie van de black box- en white box-benaderingen maakt het mogelijk om een auditomgeving systematischer te analyseren.
Het doel van het GFBS-framework is om een bepaalde laag in samenhang te analyseren. Uit de optiek van conceptuele benadering is eerst een 'geïntegreerd model' met een verzameling van neutrale auditelementen gecreëerd (zie figuur 4). Deze auditelementen behoren tot een bepaalde klasse (bijvoorbeeld beleidsklasse, procesklasse, actorklasse, et cetera) en zijn systematisch tot stand gekomen omdat ▶



Figuur 3: Projectie van de gekozen auditelementen uit een bestaand referentiekader op de lagenstructuur. Deze projectie maakt de ontbrekende auditelementen zichtbaar.



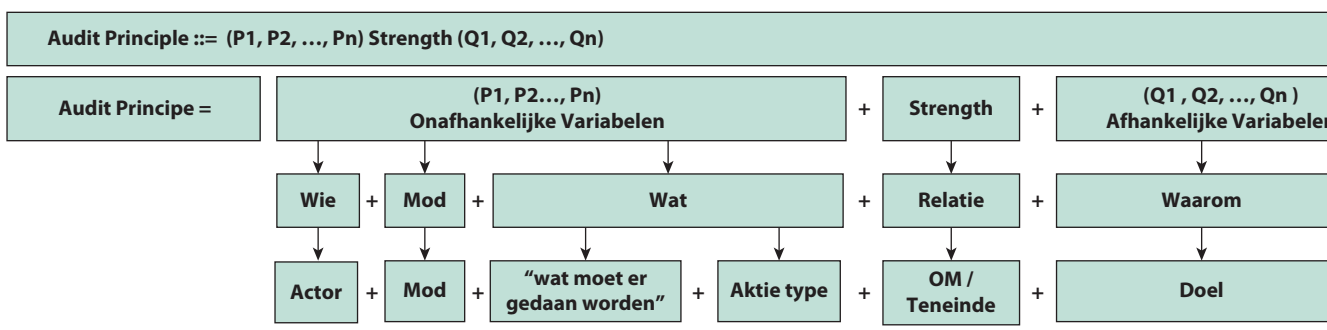
Figuur 4: Illustratie van relaties van de GFBS view en de gelijknamige modellen

elke view (G, F, B en S) zich richt op het traceren van type elementen vanuit een bepaalde invalshoek. Bij het opstellen van een referentiekader kunnen de auditelementen uit dit geïntegreerde model geprojecteerd worden op de lagenstructuur. Bij deze projectie moet per laag met vijf aspecten rekening worden gehouden: context, abstractie, perspectief van de actor, doelstellingen van de laag en de actietypen. De views houden verder het volgende in:

- Goal view. Richt zich op het waarom-aspect. Het geeft de intenties van een organisatie of doel van het product. Vanuit organisatorische invalshoek adresseert het de reden van bestaan van een organisatie. Vanuit technische invalshoek adresseert het de waarom-aspecten van een te ontwikkelen technisch apparaat. Voorbeelden van de concepten uit deze kolom zijn: enterprise, missie, visie, doelen, strategie, wetten en beleid, stakeholders en middelen.
- Function view. Richt zich op het wat-aspect. Wat geeft de acties (functies) aan die moeten worden genomen om de intenties te realiseren. Het faciliteert de identificatie van sociale, organisatorische en technologische concepten die de intenties van de organisatie zouden moeten realiseren. De technische functieview heeft betrekking op de technische functionaliteiten die door gebruikers worden geëist. Voorbeelden van de bijbehorende concepten zijn: organisatorische functies, technische functies en taken.
- Behaviour view. Richt zich op het hoe (gedrags)aspect. Het adresseert vanuit een organisatorische invalshoek de manier waarop de operationalisatie van de onderkende functies en de toegekende taken, verantwoordelijkheden en bevoegdheden aan uitvoerenden moet zijn ingericht. De technische gedragsview adresseert de manier waarop de functionele vereisten van de technische middelen, inclusief de hierbij behorende beveiligingsaspecten moeten zijn ingericht. Voorbeelden van bijbehorende concepten zijn: resources, actor, object, interactie, activiteit, toestand, eigenschap en historie.
- Structure view. Richt zich op het hoe (vorm)aspect. Het adresseert de manier waarop een organisatorische en personele structuur vorm is gegeven. De technische structuurview adresseert de manier waarop de technologische architecturen (logische en fysieke configuraties van hardware en software) vorm is gegeven. Voorbeelden van bijbehorende concepten zijn: business organisatiestructuur, IT-organisatiestructuur, business architectuur, IT-architectuur en business-IT alignment.

Form

De component Form heeft betrekking op het formuleren van auditprincipes op een consistente en eenduidige wijze op basis van een formele definitie en semi-formele syntax. Een IT-audit principe is een uitdrukking waarin relaties worden gelegd tussen onafhankelijke en afhankelijke variabelen. De onafhan-



Figuur 5: De representatie van een audit principe

kelijke variabelen in een auditprincipe vertegenwoordigen het wat-aspect en het wie-aspect. De afhankelijke variabelen vertegenwoordigen het beoogde resultaat, met andere woorden het waarom-aspect. Figuur 5 illustreert een vereenvoudigde weergave van de syntax.

- Wie: drukt de actoren uit die verantwoordelijk zijn voor de vereiste acties.
- Wat: een of meerdere acties die moeten worden uitgevoerd of een toestand die moet worden bereikt.
- Mod: drukt de modaliteiten uit: dienen, moeten en mogen en de ontkenning (*must, must not, should, should not, may en may not*).
- Strength: drukt de kracht van de motivatie uit, bijvoorbeeld *to ensure, to provide en to prove*.
- Waarom: de doelstellingen die door het principe moeten worden bereikt.

De actietypen binnen de syntax zijn verder gestandaardiseerd met behulp van de *Speech act* theorie [SEAR69; AUST62] en onderverdeeld in drie hoofdcategorieën actietypen, namelijk directieven, behabitieven en verdictieven.

- Directieven zijn groepen werkwoorden die te maken hebben met intenties, toekomstgerichtheid, het uitoefen van macht, het geven van richting, motiveren, reden om actie te ondernemen en het uitoefenen van invloed.
- Behabitieven zijn werkwoorden met betrekking tot houding en gedrag van mens en machines, het uitvoeren van acties, doen zoals het gezegd is en het brengen van veranderingen.
- Verdictieven zijn werkwoorden die te maken hebben met oordelen, uitleggen, schatten, evalueren en rapporteren.
- Deze actietypen kunnen worden gerelateerd aan de eerder genoemde abstractielagen van de lagenstructuur. Figuur 6 geeft een overzicht van de categorieën van werkwoorden, de actietypen en de lagen waarin deze actietypen van toepassing kunnen zijn.

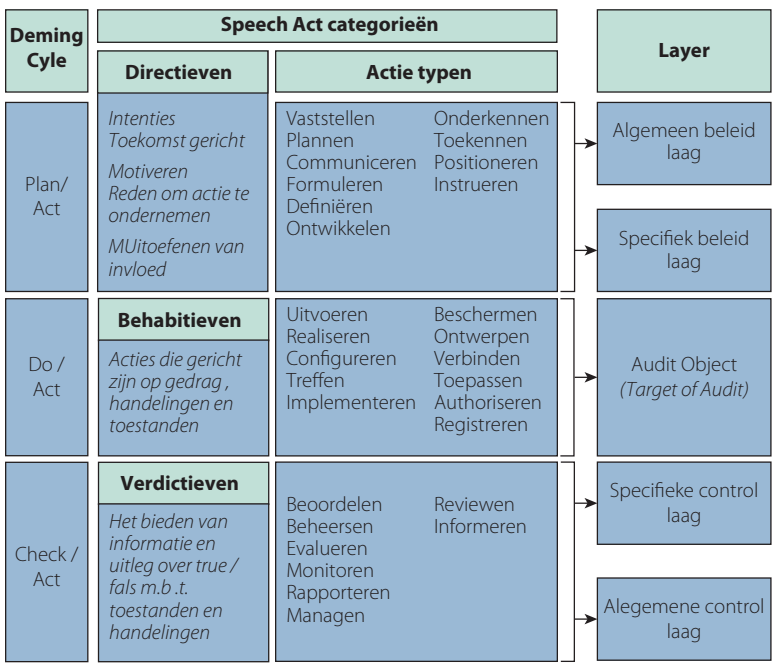
Wie	verantwoordelijke Actor
Wat	Wan services managen overeenkomstig het beleid en beveiligingsrichtlijnen,
Actietype	Managen (behoort tot de groep verdictieven)
Layer	Specifieke Control laag
Concept	IT Services
Waarom	leveren van de juiste dienst

Tabel 2: Voorbeeld

Voorbeeld: Zie Tabel 2: Voorbeeld. Stel dat de volgende norm is gedefinieerd. De vraag is op welke laag deze norm gepositioneerd moet worden.
Auditprincipe/hoofdnorm: De verantwoordelijke *Actor* voor *Wan Services* dient de Wan services te managen, overeenkomstig het specifiek beleid en beveiligingsrichtlijnen om de juiste dienst te kunnen leveren.

TOEPASSING VAN SCF-FRAMEWORK

Het gaat in dit artikel om de vraag hoe wij een referentiekader kunnen ontwikkelen op basis van dit SCF-framework. In de praktijk wordt vaak een *top-down* of een *bottom-up* benadering gehanteerd om een referentiekader te ontwikkelen. Bij de top-down benadering ontwikkelt men vanuit het hogere beleidsniveau een referentiekader. Hierbij worden, vertrekkend vanuit het top level, veelal beleids- en managementgerelateerde onderwerpen en normen geselecteerd en daarna detailnormen op het IT-gebied. Bij een bottom-up benadering besteedt men eerst aandacht aan detailnormen en pas daarna aan beleidsnormen of een mix hiervan.
De methode die in dit onderzoek wordt gehanteerd voor het systematisch ontwikkelen van een referentiekader bestaat uit drie stappen, de M3-methode, bestaande uit *Middle, Middle-out en Middle-in*.[3] Deze stappen zorgen voor een gestructureerde opzet van referentiekaders. De ▶



Figuur 6: Illustratie van relaties van de GFBS view en de gelijknamige modellen

Fases	Relaties tussen lagen
Fase 1	Analyse van auditobject vanuit de kenmerken van de IT lagen in de Middle-laag
Fase 2	Analyse van auditobject vanuit de kenmerken van Specifiek beleid (middle-out, middle-in)
Fase 3	Analyse van auditobject vanuit de kenmerken van Algemeen beleid) (middle-out, middle-in)
Fase 4	Analyse van auditobject vanuit de kenmerken van Specifieke Control (middle-out, middle-in)
Fase 5	Analyse van auditobject vanuit de kenmerken van Algemene Control (middle-out, middle-in)

Tabel 3: Overzicht van de te doorlopen fasen

M3-methode is toegepast om de valkuilen van top-down en bottom-up benadering te omzeilen. Het is een hybride-aanpak van bottom-up en top-down. Hierbij wordt het auditobject geflankeerd door twee beleidslagen en twee management- en controllagen. Eerst wordt aandacht besteed aan het auditobject zelf en daarna respectievelijk aan de beleidsnormen en management- en controlaspecten. De eerder weergegeven figuur 1 geeft een overzicht van de layers en de M3-benadering.
Bij het ontwikkelen van een referentiekader voor een auditobject kan een aantal fasen worden doorlopen. Deze fasen staan vermeld in tabel 3.
Het referentiekader wordt opgezet vanuit de Middle. Dit houdt in dat het auditobject eerst wordt verkend en de juiste concepten uit het geïntegreerd model worden geselecteerd, rekening houdend met de al eerder vermelde aspecten, zoals context, abstractie, perspectief van de actor, doelstellingen van de laag, controltype en actietypen (werkwoorden voor directieven, behabitieven en verdictieven). Richtvragen zijn bijvoorbeeld: welke IT-componenten moeten geïmplementeerd worden? Welke functies dienen te worden geleverd? Welk gedrag moeten betrokken resources vertonen? Hoe moeten de features zijn geconfigureerd? En hoe moeten de componenten zijn samengesteld?

In de overige fases is er sprake van twee routes: Middle-out en Middle-in. Deze routes worden niet separaat, maar gelijktijdig uitgevoerd. De relatie tussen deze twee fases voorziet in traceerbaarheid van de aspecten juistheid en compleetheid van concepten.
Voorbeeld: Na deze theoretische uitzetting zal een voorbeeld worden geschetst om de SCF-componenten toe te lichten. In dit voorbeeld wordt inzicht gegeven hoe een referentiekader voor een WAN (*Wide area netwerk*) kan worden aangepakt.

Structure van het Referentiekader

Ten eerste wordt vastgesteld welke lagen bij dit auditobject een rol spelen. In het SCF-framework geldt standaard dat de lagen specifiek beleid, algemeen beleid, specifieke control en algemeen control worden meegenomen, omdat het object van onderzoek altijd in deze context wordt geanalyseerd. Immers, alle auditobjecten worden in het kader van de beoordeling van het 'in control zijn' benaderd vanuit de context en vraagstelling: wat is de ist-situatie? Welke eisen en randvoorwaarden gelden hierbij (soll)? En wordt de ist-situatie beheerst op basis van evaluaties (soll versus ist)? In het SCF-framework heb je nu te maken met een dubbele beheersingscyclus omdat de beoordeling in de context van de gehele organisatie wordt bezien. Hiermee kan worden vastgesteld waar de organisatie in het geheel risico loopt. Gezien de aard van het auditobject wordt de communicatielaag in de lagenstructuur betrokken. De midden- en bovenlagen worden, vanwege eenvoud, buiten de scope gehouden. De Communicatie en de Specifieke Beleidslagen worden hieronder verder geschetst.

Content van het Referentiekader

Ten tweede wordt het Object van Onderzoek geanalyseerd vanuit de aard of van de laag waar het auditobject een rol vervult; in deze situatie is dat de communicatielaag. Bij de selectie van auditelementen uit het geïntegreerd model wordt ook rekening gehouden met de doelstelling van de desbetreffende laag en de risico's die zich per laag kunnen voordoen. Per geselecteerd auditelement kunnen auditprincipes geformuleerd worden op basis van de template. Afhankelijk van de aard van de laag (algemeen, specifiek of control) kunnen bij de formulering van de principes bepaalde actietypen gebruikt worden (zie figuur 6). In dit voorbeeld bevindt het auditobject zich op de communicatielaag en is dus operationeel van karakter. Hierbij kunnen actietypen uit de groep behabitieven gehanteerd worden.
Enkele voorbeelden van relevante auditelementen die bij technische objecten als WAN kunnen worden betrokken zijn:

Communicatie laag (Middle)

- *Goal view* – vanuit deze view kan het auditelement Procedures en richtlijnen ten behoeve van implementeren en configureren van WAN-componenten geselecteerd worden met als actietype 'toepassen'.
- *Function view* – vanuit deze view kunnen de auditelementen Taken en Taak-requirements van Wan-beheerders en Wan Services geselecteerd worden, met achtereenvolgens de actietypen 'specificeren' en 'realiseren'.
- *Behaviour view* – vanuit deze view kunnen auditelementen als Activi-

teit, Actor-Object Interactie en Object-Object Interactie, Properties, Historie, Environment, en Functionele en Non Functionele requirement geselecteerd worden met achtereenvolgens de actietypen: 'uitvoeren', 'verbinden', 'realiseren', 'registreren', 'implementeren' en 'uitvoeren'.
- *Structure view* – vanuit deze view kan het auditelement Service Architectuur geselecteerd worden met als actietypen 'configureren' en 'implementeren'.

Specifieke beleidslaag (Middle-out - Middle-in)
- *Goal view* – vanuit deze view kunnen auditelementen WAN Beleid, Stakeholder en Wan Service Beleid geselecteerd worden met als actietypen 'specificeren', 'toekennen' en 'bevatten'.
- *Function view* – vanuit deze view kunnen auditelementen Organisatorische Functie, Taken en Verantwoordelijkheden geselecteerd worden met als actietypen 'identificeren', 'vaststellen' en 'definiëren'.
- *Behaviour view* – vanuit deze view kunnen auditelementen Actor, Actor-Object Interactie en Object-Object Interactie, Properties/State, Historie en Environment geselecteerd worden met als actietypen 'toekennen', 'autoriseren', 'specificeren', 'vaststellen' en 'specificeren', 'verbinden', 'realiseren' en 'aanpassen'.
- *Structure view* – vanuit deze view kunnen auditelementen Organisatie structuur en Wan Service Architectuur met als actietypen 'vaststellen' en 'ontwerpen'.

Op dezelfde wijze kunnen ook op andere lagen auditelementen geselecteerd worden, waarover een auditprincipe geformuleerd kan worden. Wat de naamgeving van de auditelementen betreft, lijken de lagen identieke auditelementen te bevatten. Het verschil ligt in de abstractie van de lagen, perspectief van de actor, doelstellingen van de laag en actietypen. In dit voorbeeld zijn slecht de actietypen vermeld om het verschil aan te geven.

Form van auditelementen

De formulering van een auditprincipe uit dit voorbeeld ziet er dan als volgt uit:

Auditprincipe Wan Services : De <Wan specialist> <dient> de <Wan Services> te <realiseren> overeenkomstig het Wan beleid waarin eisen t.a.v. CIAA zijn gesteld <om> de juiste Wan service te kunnen leveren.

CONCLUSIE

De hoofdvraag van dit onderzoek was om een theoretisch framework en bijbehorende methode te ontwikkelen, waarmee een referentiekader op een effectieve manier en systematisch kan worden geconstrueerd. Het ontwikkelde SCF-framework en M3-methode zijn de theoretische resultaten van dit onderzoek. Deze resultaten zijn gevalideerd met twee case studies. In beide case studies zijn wij in staat geweest de tekortkomingen in verschillende referentiekaders aan te tonen. De combinatie van het SCF-framework en de M3-methode heeft enerzijds het voordeel dat deze een auditor in staat stelt de meest relevante auditprincipes te identificeren en omissies te voorkomen. Anderzijds biedt deze combinatie de auditor argumenten voor het selecteren van de auditprincipes. De selectie van auditelementen vindt plaats op basis van vijf aspecten: context, abstractie, perspectief van de actor, doelstellingen van de laag en de groepen actietypen die per laag toegepast moeten worden. De stappen die laaggewijs moeten worden doorlopen, wordt door de M3-methode aangegeven.

In dit onderzoek zijn we uitgegaan van een geïntegreerd model dat generieke auditelementen bevat, waarover auditprincipes op basis van de voorgestelde syntax zijn geformuleerd. In de praktijk zou zo een model aangevuld of vervangen kunnen worden met auditelementen die herkenbaarder zijn in de praktijk. ▶

Dr. Wiekram B.Tewarie RE is werkzaam als senior IT-auditor bij de accountantsdienst van UWV. Wiekram is betrokken bij het onderzoeksinstituut IT auditing van de Vrije Universiteit. In 2010 rondde hij zijn promotie af met de titel "Model based development of Audit Terms of Reference: a structured approach to IT auditing". Dit artikel is gebaseerd op zijn proefschrift.

Prof. dr. Ir. Ronald Paans RE is hoogleraar van de opleiding Postgraduate IT Audit aan de Vrije Univeristeit van Amsterdam en directeur van Noordbeek B.V. Ronald is voorzitter van het Wetenschapsforum voor de OV-chipkaart en voorzitter van de Raad van Toezicht van de Stichting OpenTicketing en zit onder meer in de NOREA Raad voor Beroepsethiek.

Dr. Joris Hulstijn is adviseur bij Thauris B.V. in Den Haag en universitair docent bij de faculteit Techniek, Bestuur en Management van de Technische Universiteit Delft. Hij heeft vele publicaties op het gebied van informatiesystemen en kunstmatige intelligentie.

De bovengenoemde elementen bevestigen onze werkhypothese dat een *principle-based approach* betere referentiekaders oplevert, mits het framework en de methode in voldoende mate worden begrepen en toegepast. We hopen dat de lezer de voordelen van het voorgestelde framework en de methode inziet en deze ook zal toepassen. ■

Noten

1. Het 3C-model is equivalent met het ETC (Environment, Target system en Control Organ) van De Leeuw [LEEU74]. Omwille van duidelijkheid en het voorkomen van misinterpretaties zijn de eerste twee termen vervangen door termen die door Bunge [BUNG79] wordt gehanteerd.
2. Het element S uit het GFBS-framework refereert aan de microstructuur die verband houdt met de auditelementen.
3. Middle-out kan ook worden gelezen als 'welke beleidsaspecten hebben invloed op'.
   Middle-in kan ook worden gelezen als 'welke aanvullende beleidsaspecten hebben invloed op'.

Literatuur

[AUST62] Austin, J.L., *How to do things with Words*, Cambridge, MA: Harvard Uni. Press, 1962.

[BOEH78] Boehm, B.W., Brown, J. R., Lipow, M., MacLeod, J. G., and Merritt, J. M., Characteristics of Software Quality, *TRW Series of Software Technology*, ISBN 0 4444 85105 4, 1978.

[BUNG79] Bunge, M., Treatise on Basic Philosophy, *Ontology II: A World of System*, ISBN 90-277-0944-0, Vol.4, 1979.

[IFAC2003] IFAC International Auditing and Assurance Standards Board, Proposed International Standard on Assurance Engagements (ISAE) 2000, Assurance Engagements on Subject Matters Other Than Historical Financial Information, and Proposed Withdrawal of ISA 120, Framework of International Standards on Auditing To Replace International Standard on Assurance Engagements 100, Assurance Engagements, Issued for Comment by the International Federation of Accountants, March 2003.

[LEEU74] Leeuw, A.C.J., Systeemleer en Organisatiekunde, *Een onderzoek naar mogelijke bijdragen van de systeemleer tot een integrale organisatiekunde*, Stenfert Kroese, 1974.

[STAR02], Starreveld, R.W., H.B. Leeuwen, O.C, de Mare, H. B., Joëls, E. J., *Bestuurlijke informatieverzorging*, Stenfert Kroese, ISBN 90 207 305225, 2002.

[SEAR69] Searle, J.R., Speech acts, *An essay in the philosophy of language*, Cambridge University Press, ISBN 978-0-521-09626-3 paperback, 1969.

[TEWA10] Model based development of Audit Terms of Reference: *a structured approach to IT auditing*, ISBN 978 90 8659 5358, June 2010.