ASL en CobiT, mapping van twee frameworks

Het verband tussen twee zienswijzen

Applicatiemanagementorganisaties moeten steeds vaker kunnen aantonen dat ze 'in control' zijn over hun informatieverwerkende activiteiten. Zij hanteren ASL als hulpmiddel, terwijl auditors vaak het CobiT-framework gebruiken. Wat zijn de verbanden tussen beide zienswijzen?

Machteld Meijer, Wim van 't Einde, Joep Janssen, Annita Krol

Veel organisaties moeten voldoen aan wet- en regelgeving die zegt dat de organisatie aantoonbaar 'in control' moet zijn over zijn informatievoorziening. Maakt een organisatie gebruik van applicaties, dan moet de applicatiemanagementorganisatie - of deze nou 'in huis' is of is uitbesteed - ook 'in control' zijn over de voor haar relevante aspecten. Een actueel voorbeeld is het besluit van de minister van Binnenlandse Zaken dat organisaties die DigiD gebruiken voor hun websites via een onafhankelijk ICT-beveiligingsassessment moeten aantonen dat ze 'in control' zijn over hun digitale dienstverlening aan burgers en bedrijven.

Er bestaan veel verschillende manieren om hier invulling aan te geven. In de praktijk ontstaat tussen het management van de applicatiemanagementorganisatie en de toetsende auditor regelmatig een forse discussie over het te hanteren toetskader. Daardoor kan veel tijd verloren gaan aan het krijgen van overeenstemming over de te auditen processen en de normen waaraan de processen moeten voldoen. Het resultaat van de audit is dan ook vaak niet bevredigend: niet voor de auditor, omdat de onderzochte organisatie zich niet herkent in het beeld, en niet voor de applicatiemanagementorganisatie, omdat de aanbevelingen moeilijk in te passen zijn in de bestaande processen.

Auditors hanteren steeds vaker het CobiT-framework voor het uitvoeren van audits, omdat in CobiT veel 'control objectives' (beheersingsdoelstellingen) zijn beschreven. Applicatiemanagementorganisaties hanteren steeds meer ASL als hulpmiddel voor het procesmatig inrichten van hun organisatie. Als we een verband leggen tussen de ASL-processen en de CobiT-control objectives, dan zou zowel het management van de applicatiemanagementorganisatie als de auditor erg geholpen zijn. De applicatiemanager hoeft dan niet twee afzonderlijke verbetertrajecten te starten, die in de praktijk vaak ook nog langs elkaar heen werken. Hij kan zijn processen verbeteren en bij de procesinrichting gelijk de activiteiten meenemen die nodig zijn om aan de control objectives van CobiT tegemoet te komen. De auditor ziet zijn bevindingen en aanbevelingen beter geaccepteerd worden door de applicatiemanagementorganisatie, omdat de manager hiervan de opmerkingen beter kan plaatsen.

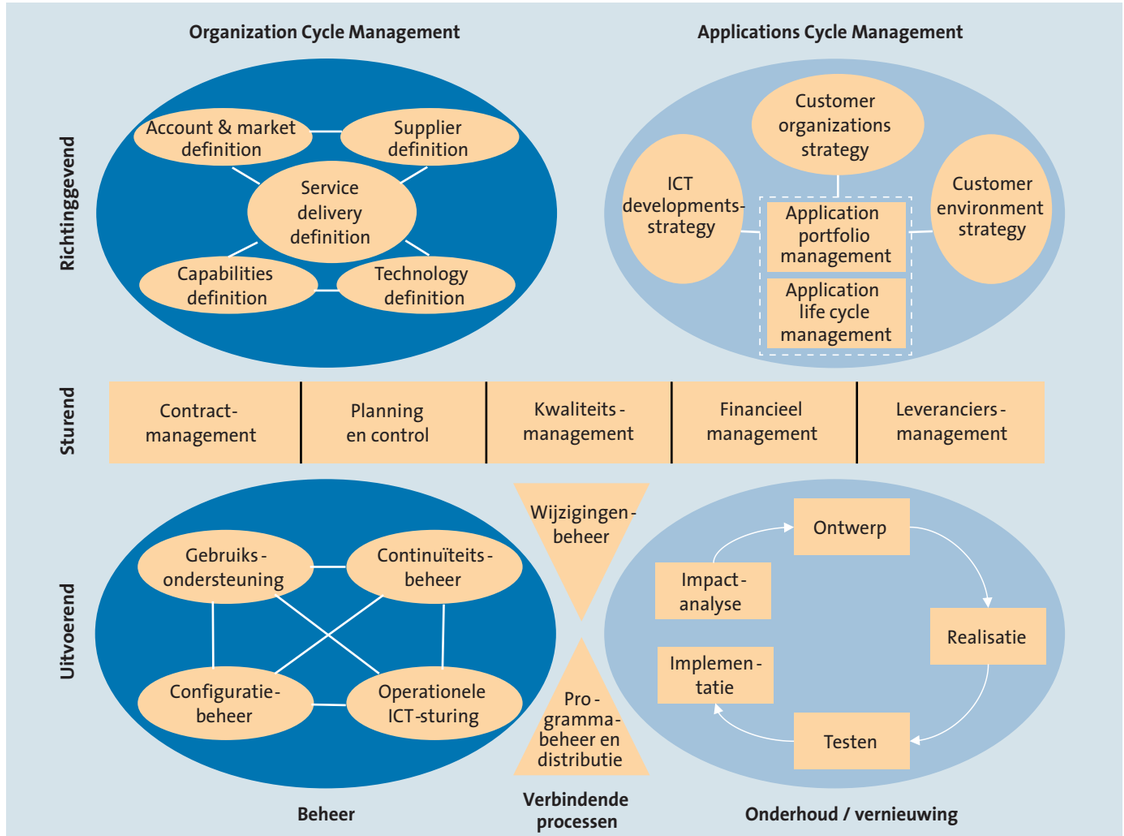
Voordat we ingaan op de verbanden tussen beide frameworks, geven we een korte uitleg van de beide frameworks.

ASL

ASL 2 heeft als doel applicatiemanagement te professionaliseren *[Pols, 2009]*. ASL wordt beheerd door de ASL BiSL Foundation en bestaat uit een framework van processen en een library van best practices op het gebied van applicatiemanagement. Applicatiemanagement wordt hier gezien in brede zin: het omvat alle processen en activiteiten die nodig zijn voor het up-to-date houden van de functionaliteit en de werking van de applicatie (de software) voor de levensduur van de ondersteunde bedrijfsprocessen.

In het framework (figuur 1), dat al eerder kort is beschreven *[Meijer, 2009]*, worden zes procesclusters onderscheiden:

- Beheer.
- Onderhoud en vernieuwing.
- Verbindende processen.
- Sturende processen.
- Organization cycle management.
- Applications cycle management.



Figuur 1 **Het ASL 2-framework**

> Tussen management en auditor ontstaat regelmatig forse discussie over het te hanteren toetskader

> Geen enkel ASL-proces heeft geen relatie met één of meerdere CobiT control objectives

De toepassingsgebieden voor ASL (applicatiemanagement) maar ook BiSL (business-informatiemanagement) zijn gebaseerd op de driedeling van beheer van Looijen (functioneel beheer, applicatiebeheer en technisch beheer). Het onderscheid tussen klant en leverancier en het belang hiervan is een uitgangspunt voor beide modellen.

CobiT

CobiT (dit was oorspronkelijk een acroniem van *Control OBjectives for Information and related Technology*) is een uitgebreid en gedetailleerd framework voor de interne beheersing van informatiegerelateerde processen (figuur 2). Het is vanaf 1992 ontwikkeld door ISACA *(Information Systems Audit and Control Association)* en ITGI *(IT Governance Institute)* en komt daarmee uit de beveiligings- en IT auditinghoek. CobiT staat vooral in de belangstelling doordat het bij uitstek geschikt is om een organisatie in staat te stellen aan te tonen dat voldaan wordt aan de regelgeving zoals die door bijvoorbeeld Sarbanes-Oxley (SOX), De Nederlandsche Bank of SAS70 wordt gevraagd. In de volgende versies van CobiT werd daarom ook steeds meer aangesloten bij control- en managementbehoeften, waardoor het framework steeds geschikter werd voor het aansturen van IT-organisaties.

De doelstelling van CobiT is om belangrijke IT-gerelateerde processen globaal te beschrijven en de belangrijkste beheersmaatregelen weer te geven. CobiT beperkt zich daarbij nadrukkelijk tot 'wat' de organisatie zou kunnen regelen en laat 'hoe' dat geregeld wordt over aan de keuze van de organisatie zelf. Frameworks als ASL, ITIL, CMMI en vele andere kunnen een nadere gedetailleerde invulling geven aan deze beheersmaatregelen. Voor de applicatiemanager kan CobiT aandachtspunten bevatten waarmee vanuit andere modellen die in de organisatie worden gebruikt wellicht geen rekening wordt gehouden. Het is overigens bij CobiT niet de bedoeling om alle processen die in het framework worden beschreven klakkeloos over te nemen. De organisatie kan het zo aanpassen dat het nauw aansluit bij de doelen van de betreffende organisatie. Risicomanagement kan hierbij een belangrijke rol spelen.

CobiT deelt de informatievoorziening van een organisatie op in vier domeinen *(Plan and Organise, Acquire and Implement, Deliver and Support en Monitor and Evaluate)*, die verder worden ingevuld door 34 processen, die op hun beurt weer zijn onderverdeeld in 208 control objectives. Het bevat daarnaast hulpmiddelen voor het meten van de 'bekwaamheid' van de 34 processen. Dat zijn 'performance drivers', kritieke succesfactoren en een volwassenheidsmodel. Het is daarmee een compleet, overzichtelijk en goed uitgewerkt hulpmiddel voor enerzijds de interne beheersing van IT-dienstverlening, maar ook voor IT-gerelateerde activiteiten aan de kant van de business.

Dat gold ook al voor CobiT-versie 4.1. Na de introductie van CobiT 4.1 ontstond meer aandacht voor waarde van IT- en risicomanagement, waardoor naast CobiT twee nieuwe frameworks ontstonden, Val-IT en Risk-IT. In het onlangs verschenen CobiT 5 zijn deze in het nieuwe framework opgenomen, waardoor de vraagkant nog meer aandacht heeft gekregen. CobiT is uitvoerig gedocumenteerd, er zijn vele tientallen boeken over CobiT verschenen, variërend van managementsamenvattingen tot zeer gedetailleerde beschrijvingen van beheersmaatregelen *(IT Governance Institute, 2007)*.

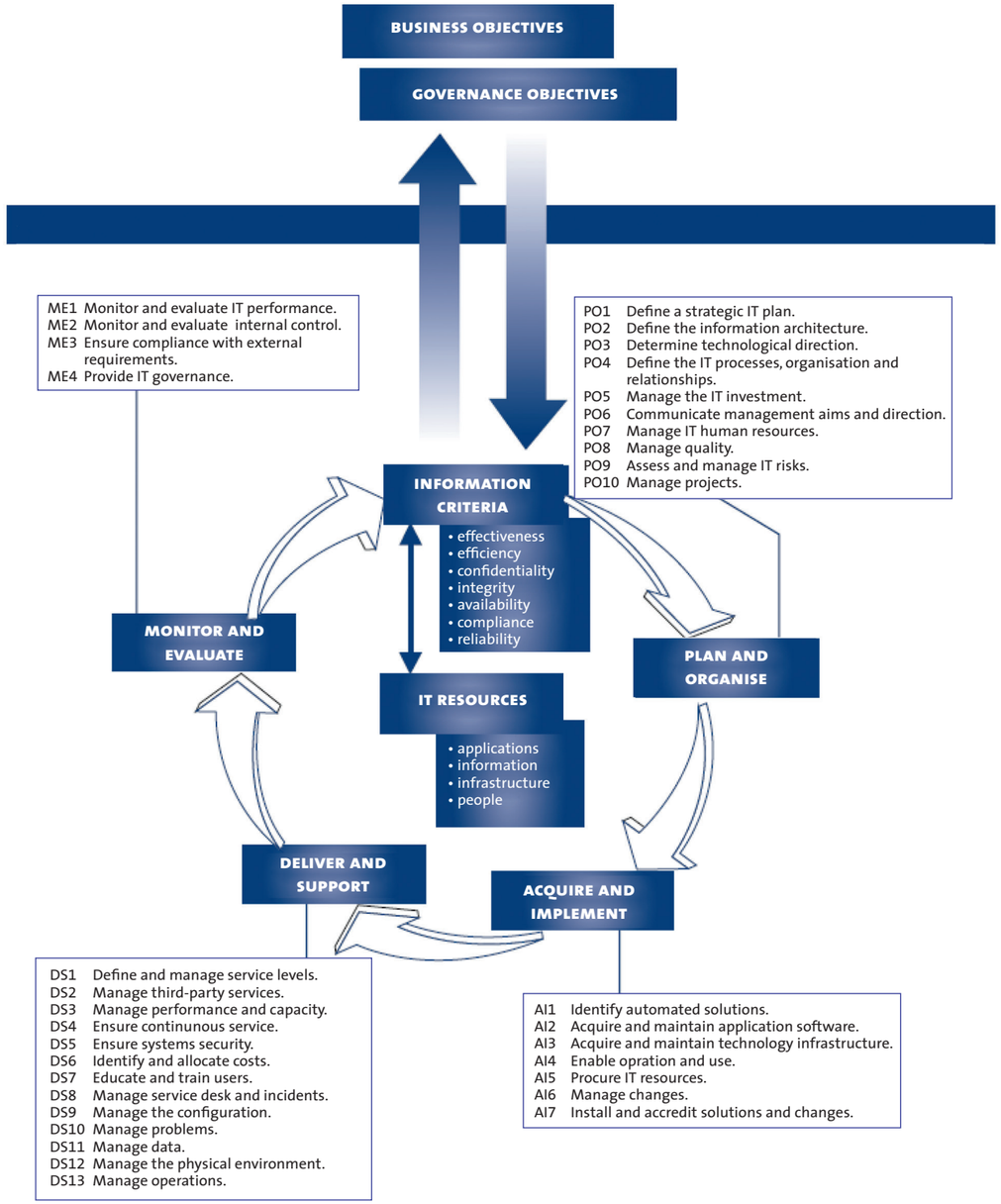
Overeenkomsten en verschillen tussen CobiT en ASL zijn via een mapping in kaart gebracht

Totstandkoming mapping

CobiT en ASL vertonen zowel overeenkomsten als verschillen. Om deze voor de gebruikers van de beide modellen in kaart te brengen, heeft een werkgroep van de ASL BiSL Foundation een mapping gemaakt. De aanleiding was dat er steeds meer vraag kwam vanuit de doelgroep van ASL om aan te geven hoe ASL hen kon helpen 'in control' te zijn en hoe ze met ASL konden voldoen aan de eisen die door de auditors – die veelal CobiT gebruikten als referentiekader – werden gehanteerd. Soortgelijke vragen werden ook gesteld over BiSL, een framework voor de vraagkant van de informatievoorziening. Omdat versie 5 van CobiT vrij lang op zich liet wachten, is versie 4.1 gebruikt als referentie. De uitbreidingen van CobiT 5 zitten meer aan de vraagkant. Dit nodigt uit om in een vervolgproject BiSL met CobiT 5 te vergelijken. In Appendix A van het framework van CobiT 5 (Enabling processes) is de link tussen CobiT 4.1 en CobiT 5 goed te leggen en daardoor indirect ook de link tussen ASL en CobiT 5.
In de mapping zijn twee zaken onderzocht:

- In hoeverre dekt een ASL-proces(gebied) de CobiT control objective af en welk proces-(gebied) is dat? Ook is meestal aangegeven welke activiteit binnen dat ASL-proces invulling geeft aan de control objectives van CobiT.
- In hoeverre dekt de CobiT control objective een proces van ASL af en welk procesgebied is dat?

Op basis van de bevindingen uit deze mapping is voor alle 208 control objectives van CobiT aangegeven in welk(e) ASL-proces(sen) deze control objectives kunnen worden ingericht. En ook is voor alle 26 ASL-processen aangegeven of en welke control objectives binnen die processen aandacht zouden moeten krijgen.



Figuur 2 **Het CobiT-framework (overgenomen uit de CobiT-documentatie)**

Control objective	Beschrijving	ASL-proces(sen)	ASL-activiteiten	In hoeverre dekt het ASL-proces de CO af	In hoeverre dekt de CO het ASL-proces af
AI2.7 Development of Application Software	Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements, and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties.	Kwaliteits-management Testen Leveranciers-management Realisatie	7.4.3 (Kwaliteitsmanagement) Opstellen kwaliteitssysteem 7.6.3 (Leveranciersmanagement) Opstellen contracten 5.5.3 (Testen) Allerlei testen 5.4.3 (Realisatie) Realiseren oplossing	A	Pp
AI4.1 Planning for Operational Solutions	Develop a plan to identify and document all technical, operational and usage aspects such that all those who will operate, use and maintain the automated solutions can exercise their responsibility.	Implementatie	5.6.3 (Implementatie) Ondersteunen bij voorbereiding verwerking en installatie 5.6.3 (Implementatie) Ondersteuning invoering in de gebruikersorganisatie	P	Pp

A = applicable; P = partly applicable; Pp = de ASL-processen bevatten meer activiteiten dan alleen deze CobiT activiteiten

Figuur 3 **Voorbeeld van Cross-reference CobiT-'control objectives' en ASL-processen en -activiteiten**

Zowel ASL als CobiT wordt ondersteund door een 'maturity-framework'. Deze zijn anders van aard en daarom in het onderzoek verder niet met elkaar vergeleken.

Globale uitkomsten

In hoeverre is ASL geschikt als kapstok om de voor een applicatiemanagementorganisatie van toepassing zijnde control objectives te implementeren? CobiT is goed in control objectives, ASL in procesinrichting. De twee frameworks kunnen elkaar aanvullen. Van alle control objectives is zo'n tweederde deel geheel of gedeeltelijk van toepassing voor een applicatiemanagementorganisatie. Aan deze control objectives wordt soms (deels) invulling gegeven door één ASL-proces, maar andere control objectives kunnen (deels) worden ingevuld door drie of vier ASL-processen.

Enkele control objectives zijn alleen van toepassing voor de business zelf. De overige die niet van toepassing zijn voor een applicatiemanagementorganisatie zijn van toepassing voor een business-informatiemanagementorganisatie (functioneelbeheerorganisatie) en/of een IT-infrastructuurmanagementorganisatie.

Aan de hand van de detailuitwerking van de cross-reference tussen de ASL-processen (en -activiteiten) en de control objectives kunnen applicatiemanagers nagaan in welke processen ze rekening zouden moeten houden met de eisen vanuit CobiT. Dat wil zeggen dat ze kunnen zien welke control objectives in welk(e) ASL-processen meegenomen kunnen worden.

De control objectives vanuit CobiT (de onderdelen van een CobiT-proces) hebben een ander karakter dan de activiteiten van ASL (de onderdelen van een ASL-proces). Binnen de ASL-literatuur kom je dan ook geen beschrijvingen tegen die overeenkomen met de control objectives en ook niet hoe je daar invulling aan zou kunnen geven. De cross-reference waarop dit artikel is gebaseerd, zou echter kunnen groeien tot een best practice als een bedrijf deze gebruikt heeft bij de implementatie van de control objectives binnen de ASL-processen.

Een voorbeeld zal een en ander verduidelijken. In figuur 3 ziet u dat control objective (CO) AI2.7 een raakvlak heeft met vier ASL-processen (via de vier genoemde ASL-activiteiten). AI4.1 raakt alleen het ASL-proces Implementatie. Wanneer een applicatiemanager ASL gaat implementeren kan hij dus bij het proces Implementatie rekening houden met (onder andere) AI4.1.

Uit de volledige matrix blijkt dat, andersom, het ASL-proces Implementatie raakvlakken heeft met zo'n acht control objectives;

> CobiT is goed in control objectives, ASL in procesinrichting. De twee frameworks kunnen elkaar aanvullen

ASL en Cobit zijn voor verschillende doelgroepen opgesteld, maar er zijn wel bruikbare relaties tussen beide frameworks

deze maken alle deel uit van een AI-proces en wel van de CobiT-processen 'Enable operation use' en 'Install and accredit solutions and changes'.

Figuur 4 legt de relatie op hoofdlijnen tussen de CobiT-processen en de ASL-processen. Hieruit komt naar voren dat de processen van ASL en CobiT vaak niet van dezelfde orde zijn. In de whitepaper wordt de volledige matrix, ASL-processen versus CobiT-control objectives, opgenomen.

In hoeverre dekt CobiT alle ASL-processen af? Er is geen enkel ASL-proces dat geen relatie heeft met één of meerdere CobiT control objectives. Uiteraard wordt aan veel control objectives invulling gegeven door het ASL-proces kwaliteitsmanagement. Voor meer dan tachtig control objectives moet in dit proces iets geregeld worden. Het zal geen verbazing wekken dat ook de processen Continuïteitsbeheer (waaronder beveiliging valt; wordt genoemd bij rond de dertig control objectives), Planning en control, Capabilities management en Financieel management een belangrijke rol spelen bij het geven van invulling aan een behoorlijk aantal control objectives (tussen de tien en twintig per proces).

De CobiT control objectives dekken de ASL-processen geen van alle geheel af. ASL beschrijft bij elk proces een aantal activiteiten die van belang zijn voor het inrichten van een applicatiemanagementorganisatie, maar waaraan geen control objective gekoppeld kan worden. Dat betekent dus dat alleen implementeren (het 'in place' hebben) van de control objectives van CobiT er niet voor zal zorgen dat een applicatiemanagement-organisatie alles goed geregeld heeft. De meeste Onderhoud- en vernieuwingsprocessen, maar ook Configuratiebeheer, worden slechts beperkt afgedekt.

Wat heeft een applicatiemanager aan de mapping? Een applicatiemanager kan bij het inrichten van zijn applicatiemanagementprocessen aan de hand van ASL in de mapping eenvoudig zien met welke control objectives hij rekening dient te houden, indien zijn organisatie geacht wordt te voldoen aan regelgeving zoals SOX en daarop geaudit gaat worden aan de hand van de CobiT control objectives. Bij een audit kan hij met de mapping aangeven door middel van welke ASL-processen hij invulling geeft aan de betreffende control objectives.

Conclusies

Hoewel ASL en CobiT voor verschillende doelgroepen zijn opgesteld, kunnen we duidelijke relaties leggen tussen beide modellen. ASL geeft een nuttige verdieping aan een deel van de control objectives van CobiT, die nauw aansluit bij de werkwijze van de applicatiemanager. Deze manager kan door de in dit artikel genoemde matrix op een eenvoudige manier de relatie tussen ASL-processen en CobiT control objectives leggen. Dit maakt het voor de applicatiemanager eenvoudiger om in CobiT-termen aan te tonen in hoeverre hij 'in control' is. Ook kan de matrix de applicatiemanager helpen bij het verbeteren van zijn processen op basis van de control objectives.

Machteld Meijer (Maise) Machteld.meijer@maise.nl, Wim van 't Einde (Belastingdienst) wimvanteinde@gmail.com, Joep Janssen (VKA) Joep.janssen@vka.nl en Annita Krol (Achmea) annita.krol@gmail.com, zijn allen lid van de werkgroep standaardisatie van de ASL BiSL Foundation.

Literatuur

IT Governance Institute, Cobit 4.1, 2007
Meijer, Machteld, ASL 2: het model is volwassener geworden, IT Beheer Magazine, 2009, nr 5.
Pols, Remko van der, ASL 2: een framework voor applicatiemanagement, Van Haren Publishing, 2009.
Whitepaper ASL and CoBIT 4.1, to be published.

	Organization cycle management					Applications cycle management					Sturende processen					Beheer				Verbind. processen		Onderhoud & vernieuwing				
	Account & market definition	Supplier definition	Service delivery definition	Capabilities definition	Technology definition	Customer organization strategy	ICTdevelopment strategy	Customer environment strategy	Application lifecycle managem.	Application portfolio managem.	Contractmanagement	Planning en control	Kwaliteitsmanagement	Financieel Management	Leveranciersmanagement	Gebruiksondersteuning	Continuïteitsbeheer	Configuratiebeheer	Operationele ICT-sturing	Wijzigingenbeheer	Programmabeheer en distributie	Impactanalyse	Ontwerp	Realisatie	Testen	Implementatie
Plan and Organise																										
PO1: Define a strategic IT plan			x	x	x	x	x	x	x	x	x	x		x												
PO2: Define the information architecture																										
PO3: Define techological direction	x	x			x	x		x	x	x			x													
PO4: Define the IT processes, organization and relationships		x	x	x							x	x	x	x	x											
PO5: Manage the IT investment				x					x	x		x		x												
PO6: Communicate management aims and direction													x		x											
PO7: Manage IT human resources				x								x	x		x											
PO8: Manage quality						x		x					x							x						
PO9: Assess and manage IT risks													x				x									
PO10: Manage projects				x								x	x	x	x					x					x	
Acquire and Implement																										
AI1: Identify automated solutions																	x					x				
AI2: Acquire and maintain application software													x		x		x		x	x	x		x	x	x	
AI3: Acquire and maintain technology infrastructure										x	x		x		x											
AI4:Enable operation use																										x
AI5: Procure IT resources		x											x		x											
AI6: Manage changes													x							x	x	x				
AI7: Install and accredit solutions and changes													x				x				x		x		x	x
Deliver and Support																										
DS1: Define and manage service levels											x		x		x				x							
DS2: Manage third-party services		x		x									x		x											
DS3: Manage performance and capacity					x								x				x		x							
DS4: Ensure continuous service				x	x								x				x									
DS5: Ensure system security																	x									
DS6: Identify and allocate costs											x			x												
DS7: Educate and train users																										
DS8: Manage service desk and incidents																x										
DS9: Manage the configuration													x					x								
DS10: Manage problems													x			x										
DS11: Manage data											x		x				x		x							
DS12: Manage the physical environment																										
DS13: Manage operations																										
Monitor and Evaluate																										
ME1: Monitor and evaluate IT performance												x	x	x												
ME2: Monitor and evaluate internal control													x													
ME3: Ensure compliance with external requirements											x		x													
ME4: Provide IT governance				x					x	x	x		x													

Figuur 4 **Cross-reference CobiT- en ASL-processen**