DE ESSENTIALS VAN CoBIT

Wat is CoBIT?

CoBIT biedt een structuur voor het inrichten van IT Governance en de daarmee samenhangende ict-organisatie en ict-architectuur. CoBIT bestaat uit een aantal good practices op het gebied van IT Governance. Deze zijn verdeeld over vierendertig ict-processen die voor elke ict-organisatie herkenbaar zijn. Binnen deze ict-processen staan beheersdoelstellingen en bijbehorende maatregelen, prestatie-indicatoren en volwassenheidsniveaus (maturity levels) centraal. CoBIT is met name gericht op beheersingsaspecten en minder op de gedetailleerde inrichting van ict-processen, zoals dat bijvoorbeeld bij itil het geval is. CoBIT maakt een aansluiting tussen de bedrijfsvoering (business requirements) en hoe ict kan worden ingezet om de bedrijfsdoelstellingen te bereiken. CoBIT richt zich meer op de wat-vraag dan de hoe-vraag. Dit betekent dat aanvullingen nodig zijn om invulling te geven aan de uit te voeren activiteiten (hoe). Hierbij is voor CoBIT aansluiting gezocht bij reeds aanwezige standaarden, zoals: COSO, itil, ISO 17799, Prince 2 en CMMI. Deze standaarden hebben zich reeds bewezen op het operationele vlak en daarom is het niet meer nodig om ook CoBIT hiermee te gaan uitbreiden. Door de aansluiting met verschillende operationele standaarden (itil, et cetera) kan worden volstaan met één standaard, wat leidt tot transparantie en overzichtelijkheid.

Wie heeft CoBIT ontwikkeld?

CoBIT staat voor Control Objectives for Information and Related Technologies. In december 2005 werd met versie 4.0 een belangrijke stap gezet door het wegnemen van de overlap met itil. Voor de verschillende aspecten op het gebied van informatiebeveiliging werd aansluiting gevonden bij de Code voor Informatiebeveiliging. Versie 4.1, gepubliceerd in december 2007, is de meest recente versie. Naast diverse detailwijzigingen (onder meer samenvoeging van verschillende Control Objectives) zijn daarin de onderdelen businessdoelen en ict-doelstellingen in appendix 1 aangepast. Het IT Governance Institute (ITGI) heeft samen met Information Systems Audit and Control Association (ISACA) aan de wieg gestaan van deze norm. ISACA is een wereldwijde organisatie voor ict-auditors. Het doel van ISACA is het onderzoeken, ontwikkelen, publiceren en promoten van een up-to-date internationaal aanvaard IT Governance-raamwerk dat managers en auditors kunnen gebruiken in hun dagelijkse werkzaamheden met betrekking tot ict-controls en -objectives. Hierbij worden het management en de proceseigenaren door middel van dit IT Governance-model ondersteund bij het begrijpen en beheersen van ict.

Voor wie is CoBIT bedoeld?

CoBIT biedt zowel de businessmanagers alsmede de ict-manager een podium om samen op trekken. Het voorziet manager, auditor en gebruikers van een set algemeen geaccepteerde meetinstrumenten, indicatoren, processen en best practices die hen kunnen helpen bij het maximaliseren van de voordelen die informatietechnologie met zich meebrengt door middel van het implementeren van een geschikte mate van IT Governance en control binnen een organisatie.

Voor het management beschrijft CoBIT waar rekening mee moet worden gehouden wanneer beslissingen over ict genomen worden en investeringen in ict worden gedaan; het helpt een balans te vinden tussen risico en investeren in controle. Het management heeft een raamwerk nodig om deze controle uit te voeren: zodat business requirements kunnen worden uitgedrukt als informatiecriteria. Dit moet dan wel een raamwerk zijn dat ict organiseert als een set

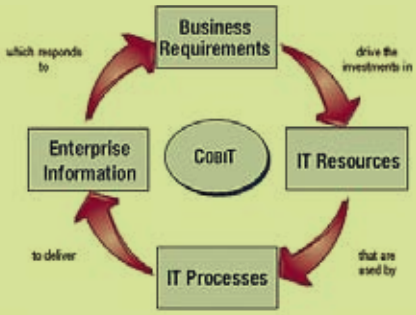
van processen en dat ict neerzet als een set van middelen. De internationaal geaccepteerde standaard als CoBIT is zo'n raamwerk. Voor auditors levert het een lijst van control objectives en minimum controls op en daarnaast een handvat voor het benchmarken van een groep; voor de gebruikers van ict geeft het een zekerheid van de beheersing van de beveiliging van de systemen.

Waarom CoBIT gebruiken?

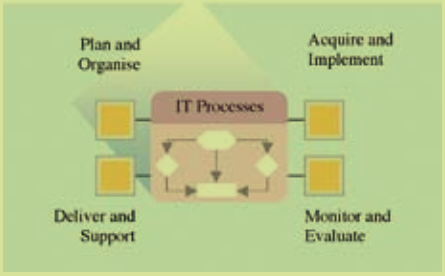
In de beginjaren van CoBIT is deze norm vooral ingezet als normenkader en te weinig als leidraad voor het implementeren van bijvoorbeeld IT Governance. Door de toenemende aandacht voor compliancy is de aandacht voor CoBIT toegenomen. Zo hebben de nodige organisaties gebruik gemaakt van CoBIT om te kunnen voldoen aan de Sarbanes Oxley-wetgeving (SOX). Op grond van deze wetgeving zijn de ondernemingen verplicht om een control statement af te geven voor alle significante processen inclusief de algemene ict-beheerprocessen.
Meer in zijn algemeenheid zijn redenen om CoBIT te implementeren:

- behoefte om IT Governance te implementeren/verbeteren;

Figuur 1. CoBIT-principe



Figuur 2. CoBIT-domeinen



Figuur 3. het CoBIT-landschap

Figuur 4. Voorbeeld van CobiT-maturitylevels

Figuur 5. CoBIT en verantwoordelijkheden en stakeholders

Stakeholders ict-management				
Managementagenda volgens CoBIT	**Primair aanspreekpunt**			
	Board	**Business Manage-ment**	**IT Manage-ment**	**Audit/ Com-pliance**
Plan and Organise				
Are IT and the business strategy in alignment? _ _	X	X	X	X
Is the enterprise achieving optimum use of its resources?	X	X	X	X
Does everyone in the organisation understand the IT objectives?	X	X	X	X
Are IT risks understood and managed		X	X	X
Is the quality of IT systems appropriate for business needs?		X	X	
Acquire and Implement				
Are new projects likely to deliver solutions that meet business needs?		X	X	
Are new projects likely to deliver on time and within budget?		X	X	
Will the new systems work properly when implemented? _		X	X	
Will changes be made without upsetting the current business operation?		X	X	
Deliver and Support				
Are IT services being delivered in line with business requirements and priorities? _	X	X	X	
Are IT costs optimised?		X	X	
Is the workforce able to use the IT systems productively and safely		X	X	
Are adequate confidentiality, integrity and availability in place?		X	X	X
Monitor				
Can IT's performance be measured, and can problems be detected before it is too late	X	X	X	
Is independent assurance needed to ensure that critical areas are operating as intended?	X			X

- ict-dienstverlening verder laten aansluiten bij de organisatiedoelstellingen;
- overnames en fusies, noodzaak tot uniformering van processen;
- standaardiseren en automatiseren van ict-processen;
- voldoen aan wet- en regelgeving (SOX, WFT, WBP, MIFID, Basel II);
- outsourcing;
- beheersbaar krijgen van ict-kosten;
- implementeren van ict-controlframework.

In alle gevallen dient gestart te worden met aansluiting te zoeken bij de organisatiedoelstellingen. Een ict-afdeling hoeft zich bijvoorbeeld niet autonoom te verantwoorden over wet- en regelgeving. Het beheersbaar krijgen van ict-kosten dient plaats te vinden in relatie tot de overall organisatiedoelstellingen.

Hoe kan een bedrijf met CoBIT gaan werken?

Het CoBIT-principe is te zien in *figuur 1*. Het startpunt van CoBIT is het definiëren of overnemen van de organisatie- en compliancydoelstellingen. Zonder deze input bestaat er geen garantie dat de navolgende stappen een bijdrage zullen leveren aan het behalen van de bedrijfsdoelstellingen. De doelstellingen worden verder uitgewerkt voor de ict-functie in vier domeinen (*zie figuur 2*):

- *Plan and Organise*, gericht op het definiëren van de ict-strategie en ict-architectuur.
- *Acquire and Implement*, gericht op het vertalen van de ict-strategie naar het implementeren van ict- oplossingen.

- *Deliver and Support*, opleveren en beheren van de geïmplementeerde oplossingen.
- *Monitor and Evaluate*, beoordelen of ict de gewenste bijdrage levert aan de bedrijfsdoelstellingen.

De vier domeinen staan met elkaar in verbinding en bestrijken het gehele ict-landschap. Beslissingen die in *Plan and Organise* worden genomen, worden in *Acquire and Implement* geïmplementeerd. In het domein *Deliver and Support* worden de deliverables in gebruik genomen door de operationele afdelingen en tegelijkertijd begint het monitoringproces om vast te stellen of de genomen beslissingen datgene opleveren wat de organisatie voor ogen had in de fase *Plan and Organise*.
Per domein zijn de bijbehorende processen gedefinieerd. De domeinen bestaan uit in totaal vierendertig processen. Eisen zijn gedefinieerd waaraan de output van ict dient te voldoen. Deze eisen zijn vertaald naar de volgende kwaliteitscriteria: effectiviteit, efficiency, confidentiality, integrity, availability, compliance en reliability. Naast de vier domeinen en kwaliteitscriteria besteedt CoBIT ook aandacht aan de te gebruiken resources. CoBIT verstaat onder resources: applicaties, informatie, infrastructuur en mensen.

CoBIT is te gebruiken ongeacht de wijze waarop de infrastructuur tot stand is gekomen. CoBIT schrijft niet voor of een organisatie gebruik dient te maken van een erp-pakket of een legacy systeem. Vanuit CoBIT kan wel worden beoordeeld of gemaakte keuzes de gewenste bijdrage leveren aan de bedrijfsdoelstellingen. Indien de uitgangspunten van een bedrijf gericht zijn op het zo veel mogelijk gebruik maken van standaardoplossingen, dan zal dat ook zichtbaar moeten zijn in de keuze van resources. In de gevallen dat de ict-afdeling van deze organisatiebreed opgezette maatwerktrajecten start, kan men zich afvragen hoe het staat met de aansluiting tussen de bedrijfs- en de ict-doelstellingen. *Figuur 3* toont de elementen van CoBIT in hun samenhang.

Hoe lang duurt een implementatie?

Het implementeren is een traject dat meestal enkele jaren kan duren, afhankelijk van de grootte van de organisatie en het gekozen startpunt. In gevallen dat CoBIT voor structuur moet zorgen in een bestaande organisatie, zal het project sneller zijn afgerond dan wanneer van scratch gestart wordt met het inrichten van een ict-organisatie. Verder moet rekening gehouden worden met het ambitieniveau (maturity level) dat wordt nagestreefd (zie *figuur 4*).

De betrokkenheid van alle stakeholders is noodzakelijk bij een implementatie van CoBIT (zie *figuur 5*). Gelet op de structuur van CoBIT is dit zeker het geval bij de aanvang van het project waarbij organisatiedoelstellingen worden vertaald naar ict-doelstellingen. Zodra de implementatie van CoBIT wordt gekwalificeerd als een typisch ict-project, dan is succes niet langer gegarandeerd.

Wanneer CoBIT implementeren?

Als zowel gebruikers als ict-medewerkers momenteel tevreden zijn over de functie van ict en de toegevoegde waarde voor de organisatie, dan is kennisname van CoBIT meer dan voldoende. In geval organisaties overwegen om aan de slag te gaan met IT Governance of om een andere reden zoals eerdergenoemd, dan is het implementeren van CoBIT het overwegen waard. CoBIT biedt een standaard die door een breed publiek wordt begrepen, inclusief auditors en toezichthouders. Bij deze twee laatste groepen zorgt CoBIT voor herkenbaarheid; daardoor begrijpen zij sneller de ict-structuur van een organisatie.

Over de auteur: **Mohamed Bouker** RE CISA is werkzaam bij de EDP Audit groep van Ernst & Young Advisory en houdt zich onder andere bezig met IT Governance en CoBIT. Dit artikel is geschreven op persoonlijke titel. De schema's zijn afkomstig uit ISACA-materiaal.