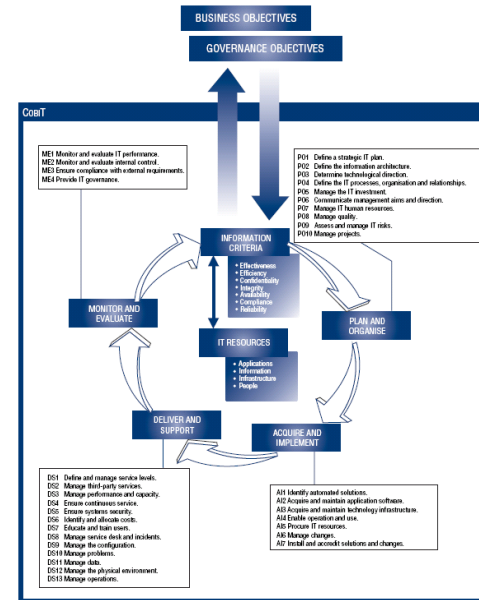


Cross reference ISM - COBIT



Auteurs: Jan van Bon, Wim Hoving
 Datum: 9 maart 2009



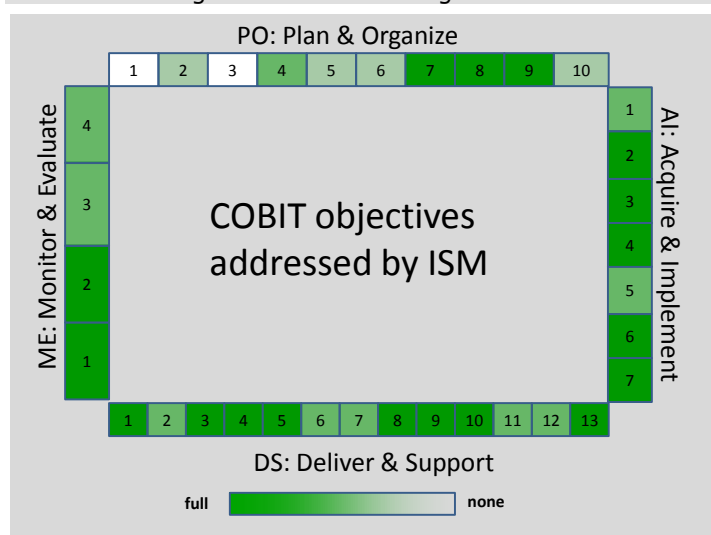
Cross reference ISM - COBIT

Management summary

Organisaties gebruiken doorgaans twee soorten instrumenten om hun prestatie te besturen: inrichtingsinstrumenten en meetinstrumenten. Met de *inrichtingsinstrumenten* wordt een organisatie vormgegeven en wordt de werkwijze bepaald en bestuurd. Met de *meetinstrumenten* wordt vervolgens onderzocht wat de prestatie van de organisatie is, tegen het licht van een vaak extern vastgestelde set van prestatiekenmerken. In deze cross-reference worden twee van dergelijke instrumenten vergeleken: ISM als instrument voor de inrichting van een IT-organisatie, en COBIT voor de analyse van de mate waarin de organisatie voorziet in een aantal belangrijke prestatiekenmerken.

ISM is een snel populair wordende standaard voor de integrale besturing van een IT-organisatie. ISM geldt als een implementatieframework waarmee complexe referentiemodellen zoals ITIL, ASL en BiSL in een organisatie kunnen worden ingevoerd. ISM is praktisch, compact, eenvoudig, en onder architectuur ontworpen. Het framework biedt een integrale besturing van de factoren proces, organisatie, en techniek. ISM integreert volledig met gangbare managementtools.

COBIT is een snel populair wordend instrument voor de analyse van een IT-organisatie. Met COBIT kan worden vastgesteld in hoeverre een organisatie voorziet in de uitvoering van een serie kerndoelstellingen ("control objectives") waaraan een goed functionerende IT-organisatie dient te voldoen. COBIT ondersteunt de inrichting van een goede IT-governance en wordt regelmatig gehanteerd als een kwaliteitstoets. Organisaties die hun opdrachtgevers moeten aantonen op verantwoorde wijze te voorzien in de informatievoorziening worden regelmatig doorgelicht tegen COBIT. De vraag in hoeverre een inrichtingsinstrument zoals ISM voorziet in de gewenste borging van de prestaties van de IT-organisatie is dus voor steeds meer organisaties van belang.



ISM is een procesmatige standaard, gericht op de operationele en tactische laag van de IT-organisatie. Hoewel er wel sprake is van processen op strategisch niveau geldt enerzijds dat deze in aanzienlijke lagere frequenties worden doorlopen, en anderzijds dat daar niet de grote uitdagingen voor IT-organisaties liggen. Veruit de meeste organisaties hebben hun handen nog jarenlang vol aan het proces- en servicegericht maken van hun organisatie.

Uit de "high-level cross-reference" blijkt dan ook dat de dekking van COBIT's control objectives door ISM zich vooral concentreert op het operationeel en tactisch niveau. ISM ondersteunt wel een groot deel van de eisen op strategisch niveau maar voorziet niet in operationele invulling daarvan, zodat de meeste strategische "control objectives" voor ISM out-of-scope zijn.

Uit de "detailed cross-reference" blijkt dat COBIT's control objectives op operationeel en tactisch niveau bijna volledig door ISM worden afgedekt. Organisaties die hun besturing en werkwijze hebben ingericht volgens ISM hebben in de praktijk dus het leeuwendeel van de COBIT-eisen voor elkaar.



Inleiding

Integrated Service Management™ (ISM) is een kwaliteitsmanagementsysteem voor IT-serviceorganisaties, waarmee de werkwijze en besturing van een IT-organisatie wordt ondersteund. Het ISM-framework bestaat uit een procesmodel, een integratie met een set van tools, een serie templates, een organisatiebeschrijving, een standaard definitiestelsel, en een implementatie-aanpak.

COBIT™ is een framework voor IT-managementorganisaties, waarin een uitgebreide serie 'control objectives' is gedocumenteerd: praktische zaken die moeten zijn geregeld wil een organisatie 'in control' zijn van haar IT. COBIT is van nature een audit-systeem, en wordt dan ook breed ingezet om te toetsen in hoeverre een IT-organisatie de vereiste beheersing heeft over deze IT.

Organisaties kunnen voor hun inrichting en besturing dus gebruik maken van ISM, en kunnen vervolgens met COBIT meten of de gewenste resultaten ook worden bereikt. Omdat beide instrumenten echter vanuit een verschillende doelstelling en historie tot stand zijn gekomen is er geen sprake van een volledige dekking. Hetzelfde geldt als er dekkingsonderzoek wordt gedaan tussen bijvoorbeeld ITIL en ISO/IEC 20000, of tussen ASL en ITIL. Het is dus van belang inzicht te krijgen in de mate waarin de beoogde instrumenten elkaar dekken. In deze paper wordt het resultaat beschreven van de dekkingsanalyse van ISM v2.0 en COBIT v4.1, een zogenaamde "cross-reference".

In eerste instantie wordt een "high-level cross-reference" beschreven. Hierin wordt aangegeven in welke mate ISM dekking geeft voor de high-level control objectives van COBIT. Deze eerste analyse geeft een goed beeld van de mate waarin beide instrumenten overlap vertonen. Vervolgens wordt een "detailed cross-reference" beschreven, waarin op elke COBIT control objective wordt ingegaan. In de analyses wordt steeds aangegeven in welke mate in de dekking wordt voorzien.

Kanttekeningen

De doelstelling van deze analyse is het verkrijgen van een antwoord op de vraag in hoeverre het hanteren van ISM voorziet in een dekking van COBIT. Ten aanzien van ISM is deze cross-reference toegepast op het ISM-procesmodel en het definitiestelsel, aangezien dat de enige 'harde' componenten zijn die door ISM zelf wordt bepaald. ISM wordt bij praktische toepassingen verder ingevuld met lokaal aanwezige tools, die vanzelfsprekend sterk kunnen variëren.

Een groot deel van de control objectives van COBIT heeft te maken met de mate waarin een organisatie iets in praktijk heeft gebracht. In de cross-reference wordt dus beschreven welke dekking ISM biedt, mits de organisatie die van ISM gebruik maakt ook daadwerkelijk de ISM-werkwijze in de praktijk brengt. Om vast te stellen of een organisatie de in ISM gespecificeerde werkwijze daadwerkelijk in praktijk brengt zal de organisatie bewijsstukken moeten kunnen overleggen. Hieronder vallen bijvoorbeeld de in ISM genoemde documenten, zoals een SLA, een Service Catalog, een RFC-formulier, et cetera. In die documenten dient dan de concrete dekking van de in ISM genoemde aspecten te zijn toegepast.

ISM is een discreet model en kent dus geen maturitylevels. We kunnen dus uitsluitend vaststellen in hoeverre ISM voorziet in elementen van elk van de te onderzoeken aspecten.

High level cross-reference

Bij de high-level cross-reference is aangegeven hoe de dekking van ISM is t.a.v. de high-level control objectives. Uit de navolgende figuur volgt dat ISM een lichte dekking heeft in het PO-domein, een sterke dekking in het AI-domein, een volledige dekking in het DS-domein, en een bijna volledige dekking in het ME-domein.

De dekking door ISM is in de cross-reference gecategoriseerd volgens een systeem van 4 niveaus:

1. **Completely covered** – ISM voorziet volledig en expliciet in de betreffende karakteristiek
2. **Largely covered** – ISM voorziet in de karakteristiek, maar invullingen kunnen in detail afhankelijk zijn van wat de organisatie er in de praktijk van maakt
3. **Supported** – ISM zelf voorziet niet in de karakteristiek, maar biedt wel structuren die als ondersteuning daarvoor kunnen dienen
4. **Not explicitly covered** – karakteristieken die buiten de scope van ISM vallen

High level dekking van COBIT door ISM

Domain	High level objective in COBIT 4.1	High-level coverage in ISM: 1-2-3-4			
		LEGEND			
		COMPLETELY COVERED, explicit	LARGELY COVERED, sometimes more implicit than explicit	SUPPORTED, but often a responsibility of the local organization	NOT EXPLICITLY COVERED
Plan and Organise	PO1 Define a strategic IT plan				
	PO2 Define the information architecture				
	PO3 Determine technological direction				
	PO4 Define the IT processes, organisation and relationships				
	PO5 Manage the IT investment				
	PO6 Communicate management aims and direction				
	PO7 Manage IT human resources				
	PO8 Manage quality				
	PO9 Assess and manage IT risks				
	PO10 Manage projects				
Acquire and Implement	AI1 Identify automated solutions				
	AI2 Acquire and maintain application software				
	AI3 Acquire and maintain technology infrastructure				
	AI4 Enable operation and use				
	AI5 Procure IT resources				
	AI6 Manage changes				

	AI7 Install and accredit solutions and changes			
Deliver and Support	DS1 Define and manage service levels			
	DS2 Manage third-party services			
	DS3 Manage performance and capacity			
	DS4 Ensure continuous service			
	DS5 Ensure systems security			
	DS6 Identify and allocate costs			
	DS7 Educate and train users			
	DS8 Manage service desk and incidents			
	DS9 Manage the configuration			
	DS10 Manage problems			
	DS11 Manage data			
	DS12 Manage the physical environment			
	DS13 Manage operations			
Monitor and Evaluate	ME1 Monitor and evaluate IT performance			
	ME2 Monitor and evaluate internal control			
	ME3 Ensure compliance with external requirements			
	ME4 Provide IT governance			