Wet- en regelgeving levert een duidelijke business case

SOX en Code Tabaksblat: tijd voor identity management?

Identity management (IdM) staat nationaal en internationaal hoog op de agenda van vrijwel elke IT-manager, vooral als gevolg van de komst van wet- en regelgeving zoals Sarbanes-Oxley (SOX) en Code Tabaksblat. Bart de Best beschrijft de invloed die SOX en de Code Tabaksblat hebben op beheerorganisaties en onderzoekt de business case voor IdM.

Bart de Best

Zoals gebruikelijk in de ICT-wereld wordt het begrip IdM op diverse manieren gedefinieerd en gehanteerd. In dit artikel wordt IdM gezien als een beheerproces. Als uitgangspunt hanteren we de definitie van KPMG: 'Het beleid, de processen en de ondersteunende systemen die managen welke personen toegang verkrijgen tot informatie en ICT-middelen en wat ieder persoon gerechtigd is hiermee te doen.'

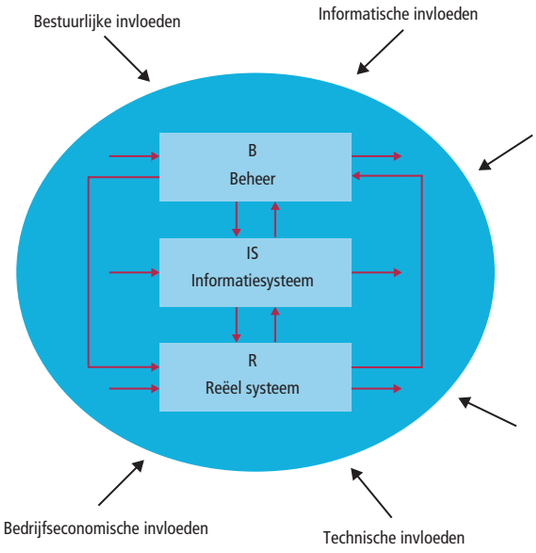
IdM omvat twee aandachtsgebieden, te weten *user lifecycle management* en *access management*. Onder user lifecycle management vallen taken zoals het aanmaken van accounts, het beheer van gebruikersgegevens en het verwijderen van gebruikers. Access management houdt zich bezig met het definiëren van rechten en het authentiseren en autoriseren van gebruikers voor de toegang tot en de mutatie van gegevens en het uitvoeren van programma's. Beide worden in relatie gebracht met SOX en de Code Tabaksblat. Tevens wordt stilgestaan bij de rol van access management in het kader van de nieuwe Nederlandse wet Bevoegdheden vorderen gegevens.

Probleemstelling

In de vele publicaties over dit onderwerp en in reclamecampagnes door leveranciers wordt de relatie tussen wet– en regelgeving en IdM niet scherp gedefinieerd. Laat staan dat ze op basis van deze wet– en regelgeving een business case voor IdM hard maken. Tijd dus om eens stil te staan bij deze veronderstelde business case en vast te stellen of deze wel zo significant is. En zo ja, te onderzoeken in welke mate IdM de beheerorganisaties dan verder helpt.

Nieuwe rubriek: Topic

Topic is een nieuwe rubriek in *IT Beheer Magazine*, waarin een actuele ontwikkeling of een belangrijk onderdeel van het vakgebied diepgaand wordt belicht.



Figuur 1 Beheerparadigma

Om maar dicht bij huis te beginnen zullen we IdM zo veel mogelijk afbeelden op de meest gangbare beheermodellen. Hiertoe wordt het beheerparadigma van Looijen[1] gehanteerd, zoals afgebeeld in figuur 1. Hierin is te zien dat de bedrijfsprocessen (R) gebruikmaken van informatiesystemen (IS) om informatie op te slaan en te bewerken. Het beheer (B) bewaakt dat de informatiesystemen aan de juiste kwaliteitseisen en kwantiteitseisen voldoen.

Aan de hand van de drie componenten (R, IS en B) van het beheerparadigma worden eerst SOX en de Code Tabaksblat besproken en de consequenties die deze wet- en regelgeving voor organisaties heeft (R). Daarna wordt de rol van de informatiesystemen hierin geschetst (IS). Ten slotte wordt met een combinatie van de COSO- en CobiT-modellen aangegeven op welke wijze IdM invulling geeft aan de gestelde eisen (B).

Reëel systeem (R)

De blauwe cirkel in figuur 1 staat symbool voor een willekeurige organisatie die in haar bedrijfsvoering wordt beïnvloed door de buitenwereld (de zwarte pijlen). Zo vereisen de globalisering en e-commerce steeds intensievere informatieoverdracht tussen bedrijven en hun klanten, tussen bedrijven en de overheid en tussen bedrijven onderling. Op het gebied van IdM moeten hiertoe de nodige technische voorzieningen worden getroffen. Denk aan de koppeling van een organisatie met DigiD (voorheen de Nationale Authenticatie Voorziening).

Een ander voorbeeld van externe beïnvloeding is wetgeving zoals SOX in de Verenigde Staten. De evenknie in Nederland is de regelgeving van de Code Tabaksblat. Beide stellen dat aan de beurs genoteerde organisaties *in control* moeten zijn, mede ingegeven door misstanden die in het verleden hebben plaatsgevonden bij grote beursgenoteerde bedrijven zoals het Amerikaanse bedrijf Enron. Daarnaast zijn er natuurlijk vele andere nationale en internationale wet- en regelgevingen waar steeds meer organisaties rekening mee moeten houden zoals Basel II, Wet bescherming persoonsgegevens (Wbp), Health Insurance Portability and Accountability Act (HIPAA) en Wet bevoegdheden vorderen gegevens. De sancties die op basis van het niet nakomen van de SOX-wetgeving kunnen worden opgelegd, liegen er niet om en treffen het bestuur van betrokken organisaties persoonlijk. Veel bedrijven zijn dan ook naarstig op zoek gegaan hoe zij zo objectief mogelijk kunnen aantonen dat zij voldoen aan deze wetgeving.

De vraag is echter in hoeverre SOX en de Code Tabaksblat nu voorschrijven dat er maatregelen moeten worden getroffen in de ICT-sfeer, in casu IdM. Het antwoord is simpel: ze zeggen daar niets over. Een recent onderzoek van Gartner stelt zelfs dat 33% van de organisaties in de Verenigde Staten geen reden ziet om de ICT-afdeling te betrekken in het onderzoek naar SOX-*compliance*. In Nederland lijkt een nog hoger percentage geen ICT-paragraaf op te nemen in de jaarlijkse rapportage van de Code Tabaksblat. Toch onderkent de meerderheid van de bedrijven *wel* een impact van de wet- en regelgeving op de ICT-voorzieningen. De vraag is dan ook *welke* directe of indirecte relaties onderkend worden. Laten we eerst even stilstaan bij de wet- en regelgeving, te beginnen met de SOX-wet.

Sarbanes-Oxley

De belangrijkste secties van SOX die betrekking hebben op de ICT-dienstverlening zijn deze:

- Section 103: alle aan de audit gerelateerde gegevens moeten zeven jaar worden vastgehouden – dit betreft dus ook gegevensbestanden.
  → *Dit heeft niet alleen een impact op de bewaartijd van tapes. Als u nieuwe informatiesystemen gebruikt, zult u omwille van de bewaartijd van zeven jaar ook de oude informatiesystemen moeten kunnen herstellen of de oude data converteren.*
- Section 201: auditbedrijven mogen geen IT-gerelateerde services bieden.
  → *Uiteraard heeft dit consequenties voor zowel klanten als leveranciers. Beide zullen moeten kijken naar de*

Het COSO-framework

De doelstelling van het COSO-model is om bedrijven winstgevend te houden, om bedrijven hun doelstellingen te laten halen en om verrassingen te minimaliseren. Het COSO-model geeft een invulling aan het 'in control' zijn door het definiëren van een framework van internal controls. COSO definieert een internal control als volgt:

A process effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of the objectives in the following categories:
- *Effectiveness and efficiency of operations*
- *Reliability of financial reporting*
- *Compliance with applicable laws and regulations*
- *Safeguarding of assets (added later)*

Het COSO Internal Control Integrated Framework bestaat uit vijf componenten. Hieronder zijn deze componenten in het kort beschreven aan de hand van de *entity level controls*. (Dit is het hoogste niveau waarop gemeten kan worden, lagere niveaus zijn proces-, transactie- en applicatieniveau.)

1. Control environment
   - Integrity & Ethical Values (DS1, DS2)
   - Commitment to Competence
   - Board of Directors or Audit Committee
   - Management's Philosophy and Operation Style
   - Organizational Structure
   - Assignment of Authority and Responsibility
   - Human Resource Policies and Practices
2. Risk assessment
   - Objectives
   - Risk Identification & Analysis (DS2)
   - Management Change (DS2)
3. Control activities
   - Policies & Procedures (AI4, AI6, DS1, DS2, DS9, DS10, DS11, DS12)
   - Information System Controls (AI2, AI3, AI5, DS5, DS11, DS13)
   - Entity Specific Controls
4. Information and communication
   - Information (AI4, DS5, DS9, DS10, DS11, DS13)
   - Communication
5. Monitoring
   - Ongoing Monitoring (AI6, DS1, DS2, DS5, DS10)
   - Separate Evaluations
   - Reporting Deficiencies

(Ontleend aan de publicatie van de Office of Internal Auditing[2]. Tussen haakjes zijn de relaties met CobiT aangegeven.)

impact van deze veranderingen op hun contracten.
- Section 301: medewerkers moeten confidentieel en anoniem klachten kunnen melden aan de auditcommissie.
  → *Dit heeft alleen een procedurele impact.*
- Section 302: CEO/CFO moet de accuraatheid en tijdigheid van de financiële rapportage aantonen.
  → *Bij een handmatige rapportage wordt dit erg lastig.*

  Tevens moeten de significante gebreken van de *internal controls* worden gemeld aan de auditcommissie en de externe auditors.
  → *Dit vereist voor ICT in ieder geval een goed incident management process.*
- Section 404: CEO/CFO en auditors moeten de effectiviteit van interne controls voor de financiële rapportage bevestigen.
  → *Dit wordt gezien als de belangrijkste grondslag voor betrokkenheid van ICT.*

  Het management moet de effectiviteit van de internal controls testen.
  → *Dit ligt dicht in de buurt van een CobiT- of ITIL-audit.*
- Section 409: *Real time* kunnen aantonen van wijzigingen in de financiële status; 'Real time' kan natuurlijk alleen met informatiesystemen.
  → *Dit is na section 404 de belangrijkste sectie die wijst op de relatie met ICT.*
- Section 802: audit en gerelateerde documenten moeten beschermd worden en terug te lezen zijn, inclusief de elektronische gegevens.
  → *Let wel: dit betekent tevens dat als u overgaat van SAP naar bijvoorbeeld Siebel, u dus beide systemen moeten blijven supporten (mensen en middelen) of moet converteren. De conversie moet dan natuurlijk goedgekeurd worden door een audit.*
- Section 906: CEO/CFO moet de accuraatheid van de financiële rapportage aantonen (*certify*).
  → *Ook dit punt is lastig te realiseren zonder ICT.*

Het meest significant is section 404. De reden is dat de meeste risk managers in de VS onderkennen dat de gegevens die gebruikt worden om tot de financiele rapportage te komen, net zo goed beschermd moeten zijn door internal controls als de financiële rapportage zelf. Dit omvat niet alleen de gegevensbestanden maar ook de informatiesystemen en de infrastructuur. De meeste bedrijven in de VS kiezen voor de risicobeheersing het COSO-framework (zie het gelijknamige kader) in combinatie met CobiT (dat hierna aan de orde komt). Dit is mede ingegeven door het feit dat de SEC (Securities and Exchange Commission) de keuze van COSO adviseert.

Code Tabaksblat

Belangrijk voor de IdM business case is de concreetheid van de wet– en regelgeving. Helaas is de Code Tabaksblat wat dat betreft nog minder concreet dan SOX en tevens veel vrijblijvender. Waar SOX

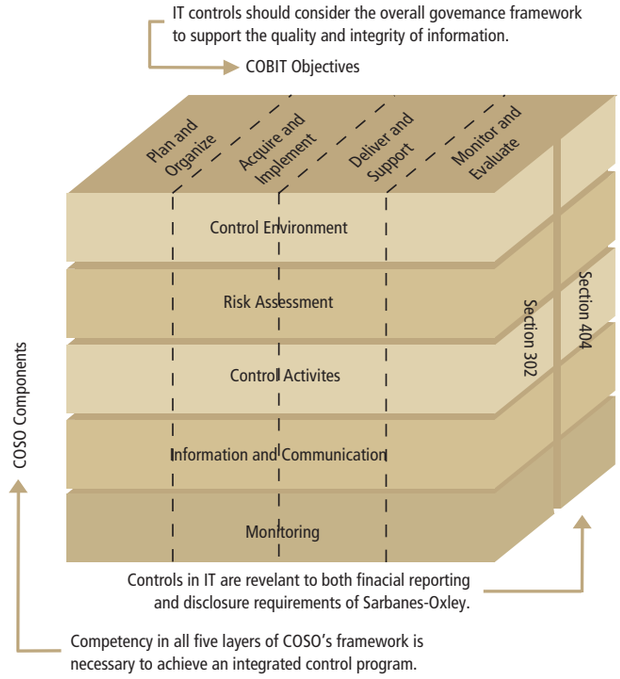
nog verwijst naar algemeen aanvaarde systemen om 'in control' te komen, verwijst de Code Tabaksblat alleen in de toelichting naar COSO (Toelichting II 1.4.).
Ook stelt de Code Tabaksblat geen vereisten aan het formaat van de financiële verslaglegging. Verder komt de vrijblijvendheid tot uitdrukking in het ontbreken van sancties. De Code Tabaksblat is tenslotte een aanbeveling en geen wet, maar is wel middels een Algemene Maatregel van Bestuur in de wetgeving verankerd.
Deze vergelijking met SOX wil overigens niet zeggen dat de Code Tabaksblat beter of slechter is. Beide hebben echter een andere herkomst en zijn gebaseerd op verschillende uitgangspunten qua cultuur en overige wetgeving.

Overigens is de Code Tabaksblat breder in zijn vereisten. Zo is het management niet alleen verantwoordelijk voor de financiële rapportage maar moet het zich ook verantwoorden ten aanzien van de operationele risico's. De vrijblijvendheid van de Code Tabaksblat blijkt uit twee preambules van deze regelgeving, te weten:

- Preambule 5: "De principes zijn uitgewerkt in concrete best practice bepalingen. Deze bepalingen creëren een zekere normstelling voor het gedrag van bestuurders en commissarissen – ook in relatie tot de externe accountant – en aandeelhouders. Zij geven de nationale en internationale 'best practice' weer en kunnen worden opgevat als een nadere invulling van de algemene beginselen van goede corporate governance. Beursgenoteerde vennootschappen kunnen hiervan afwijken. Afwijkingen zijn op zich niet verwerpelijk; zij kunnen onder omstandigheden juist gerechtvaardigd zijn."
- Preambule 6: "In internationale regelgeving en codes wordt de flexibiliteit in zoverre aan banden gelegd door beursgenoteerde vennootschapbedrijven te verplichten elk jaar in hun jaarverslag gemotiveerd uit te leggen of en zo ja waarom en in hoeverre zij afwijken van de best practice bepalingen van de corporate governance code (de regel van 'pas toe of leg uit')."

In de Code Tabaksblat zijn wel de volgende aan IT gerelateerde best practices te onderkennen:

- **II.1.3.** In de vennootschap is een op de vennootschap toegesneden intern risicobeheersing- en controlesysteem aanwezig. Als instrumenten van het interne risicobeheersing- en controlesysteem hanteert de vennootschap in ieder geval:
  a. risicoanalyses van de operationele en financiële doelstellingen van de vennootschap;
  b. een gedragscode die in ieder geval op de website van de vennootschap wordt geplaatst;
  c. handleidingen voor de inrichting van de financiële verslaglegging en de voor de opstelling daarvan te volgen procedures;
  d. een systeem van monitoring en rapportering.
  → *Onder punt a vallen tevens de risicoanalyses van de operationele doelstellingen. Hierdoor is de Code Tabaksblat breder georiënteerd dan SOX! Hier spelen beheerprocessen en daarmee ook IdM een belangrijke rol.*
- **II.1.4.** In het jaarverslag verklaart het bestuur dat het interne risicobeheersing– en controlesysteem adequaat en effectief is en geeft een duidelijke onderbouwing hiervan.



Figuur 2 Relatie tussen COSO en CobiT (bron: ISACA)

→ *Deze 'best practice' wordt als belangrijkste voor de ICT beschouwd. Het onderbouwen dat voldaan wordt aan deze eis voert wel ver, zeker omdat dit dus ook de operationele processen betreft.*

- **V.4.3.** Het verslag van de externe accountant ingevolge artikel 2:393 lid 4 BW bevat datgene wat de externe accountant met betrekking tot zijn controle van de jaarrekening en de daaraan gerelateerde controles onder de aandacht van het bestuur en de raad van commissarissen wil brengen. Daarbij kan aan de volgende onderwerpen worden gedacht:
  V.4.3.C. "Met betrekking tot de werking van het interne risicobeheersing- en controlesysteem (inclusief de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking) en de kwaliteit van de interne informatievoorziening:
  – verbeterpunten, geconstateerde leemten en kwaliteitsbeoordelingen;
  – opmerkingen over bedreigingen en risico's voor de vennootschap en de wijze waarop daarover in te publiceren gegevens gerapporteerd dient te worden;
  – naleving van statuten, instructies, regelgeving, leveringsconvenanten, vereisten van externe toezichthouders, etc."
  → *De Code Tabaksblat geeft hier een directe relatie naar betrouwbaarheid en continuïteit van informatiesystemen en hanteert daarbij zelfs het woord 'geautomatiseerde'. Continuïteit is hierbij wederom een stap verder dan SOX gaat. In de VS wordt momenteel vanuit auditingkringen geopperd om de continuïteit niet te betrekken in de SOX-rapportage.*

Wet bevoegdheden vorderen gegevens

Naast SOX en de Code Tabaksblat hebben de overige eerdergenoemde wet- en regelgevingen een enorme impact op de betrokken beheerorganisaties. Zo geeft de recent aangenomen Wet bevoegdheden vorderen gegevens vergaande bevoegdheden aan de overheid. Niet alleen het vorderen van identiteitsgegevens wordt mogelijk gemaakt, maar ook onder meer alle informatie met betrekking tot gegevensmanipulatie en internetgebruik. Een organisatie moet hiertoe dus al het dataverkeer gaan bewaken, opslaan en bewaren. Gelukkig bieden steeds meer IdM-leveranciers hiertoe functionaliteit in hun tools. We beperken ons hier wat betreft de business case voor IdM tot SOX en de Code Tabaksblat.

Informatiesystemen (IS)

De wetgever stelt dus aangescherpte eisen aan risicobeheersing en rapportage ten aanzien van de bedrijfsprocessen, met als focus de financiële verslaglegging. Dit heeft indirect impact op de bestaande informatiesystemen (zie figuur 1) die door de bedrijfsprocessen worden gebruikt en op basis waarvan de financiële rapportage wordt samengesteld. Informatiesystemen vormen in het beheerparadigma feitelijk het geheugen van de bedrijfsprocessen als het gaat om informatievoorziening. Daarnaast vormen de informatiesystemen het brein van de bedrijfsprocessen in de zin van de immense rekenkracht waarmee de opgeslagen informatie wordt getransformeerd en verrijkt. Tot slot vormen de informatiesystemen en de onderliggende infrastructuur een enorm communicatiekanaal. Zonder dit kanaal zijn de meeste bedrijven binnen enkele dagen failliet.

Het 'in control' zijn van de bedrijfsprocessen komt dan ook in grote mate neer op het 'in control' zijn van die informatiesystemen, zoals kunnen aangeven:

- hoe de beveiliging van de informatie is geregeld;
- wie toegang heeft tot welke informatie;
- wie welke informatie mag muteren;
- wie toegang heeft tot de informatie die is opgeslagen in die informatiesystemen (authenticatie & autorisatie);
- dat de informatie uit elektronische archieven is terug te halen;
- dat er een financiële rapportage is die aangeeft dat de boekhouding Juist, Volledig, Tijdig en Accuraat is (JuVoTA);
- waar de data wordt opgeslagen;
- wat er met deze data wordt gedaan, inclusief audittrails.

CobiT processen		COSO					PCAOB IT General Control Heading			
		Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring	Program Development	Program changes	Computer operations	Access to program and data
ACQUISITION & IMPLEMENTATION										
AI2	Acquire and Maintain Application Software			X			X	X	X	X
AI3	Acquire and Maintain Technology Infrastructure			X			X	X	X	
AI4	Develop and Maintain Procedures			X	X		X	X	X	X
AI5	Install and test application software and technology infrastructure			X			X	X	X	X
AI6	Manage Changes			X		X		X		X
DELIVERY & SUPPORT										
DS1	Define and Manage Service Levels	X		X		X	X	X	X	X
DS2	Manage Third-Party Services	X	X	X		X	X	X	X	X
DS5	Ensure Systems Security			X	X	X			X	X
DS9	Manage the Configuration			X	X				X	X
DS10	Manage Problems and Incidents			X	X	X			X	
DS11	Manage Data			X	X				X	X
DS13	Manage Operations			X	X				X	X

Tabel 1 Relatie tussen CobiT en COSO- en PCAOB-controls (bron: ISACA)

Bij het realiseren van de internal controls van COSO is voor de ICT dan ook een belangrijke rol weggelegd. Hierbij voeren de beheersing en het beheer van de ICT-middelen de boventoon, al was het alleen al vanuit beveiligingsoptiek. IdM-producten zijn een goed hulpmiddel bij zowel het inregelen van als het rapporteren over de bovenstaande vereisten.

IdM-producten zijn informatiesystemen op zich. Ze bevatten immers informatie over personen, rollen, rechten, enzovoort. Ze zijn echter ondersteunend aan beheertaken en worden daarom niet afgebeeld op deze component (IS) van het beheerparadigma, maar op de beheercomponent (B).

Beheer (B)

Het COSO-model biedt dus een mogelijkheid om te bepalen of een organisatie 'in control' is. De vraag is nu hoe je vaststelt of je *compliant* bent. Hiertoe moeten we dus op zoek naar een meetmethode. Willen we de business case voor IdM kunnen invullen, dan moet vanuit deze meetmethode (audit) tevens een relatie te leggen zijn naar IdM. ITIL biedt zo'n meetmethode[4]. Deze meetmethode biedt echter niet een afdoende dekkingsgraad voor de COSO-aspecten. Een meetmethode die COSO wel goed afdekt is CobiT. CobiT wordt veel gebruikt in de VS en mondjesmaat in Nederland. CobiT is overigens geen vervanger van ITIL, deze modellen zijn juist veeleer complementair. Bovendien is CobiT geen verbetermodel maar een meetmodel. CobiT beschrijft op basis van vier domeinen in totaal 34 processen die weer in totaal 318 controls bevatten. ISACA (Information Systems Audit and Control Association) heeft de relatie tussen beide modellen onderkend (zie figuur 2).

Duidelijk is in figuur 2 te zien dat alle COSO-componenten een relatie hebben met alle vier de CobiT-domeinen en de 34 processen daarbinnen. Deze figuur wordt vaak gebruikt in publicaties, maar legt de vinger niet op de zere plek. Om te achterhalen op welke wijze een beheerorganisatie invulling kan geven aan SOX en de Code Tabaksblat, moeten we inzoomen op deze kubus, zoals weergegeven in tabel 1. Binnen de scope zoals gedefinieerd in tabel 1 gaan we op zoek naar de business case voor IdM.

In tabel 1 heeft ISACA niet alleen een concretere invulling gegeven aan de relatie tussen COSO en CobiT, maar heeft zij tevens de relatie met PCAOB-aandachtsgebieden gelegd. De PCAOB (Public Accounting Oversight Board) is een orgaan dat toezicht houdt op en richtlijnen geeft aan de externe auditors die bij bedrijven de SOX-compliance bepalen. In tabel 1 zijn alleen die CobiT-processen weergegeven die voor het 'in control' zijn van de IT-organisatie van belang zijn. Deze CobiT-processen zijn uitgezet tegenover de COSO-componenten en tevens tegenover de PCAOB-aandachtsgebieden. Om de business case voor IdM nog verder af te bakenen zijn de cellen gekleurd. Alleen de witte cellen zijn van belang voor IdM. Tot de keuze van kleuring van de cellen is als volgt gekomen:

- PCAOB: de relatie van de vier PCAOB-aandachtsgebieden met de CobiT-processen geeft een indicatie van belangrijke controlepunten. Voor de business case van IdM is alleen 'Access to program and data' van belang. Hiermee komen dus de CobiT-processen AI3 en DS10 te vervallen als onderdeel van de business case. Deze zijn dan ook blauw gekleurd.
- CobiT: vanuit het CobiT-model zelf is ook een afbakening te geven voor IdM. Dit is gedaan door per

CobiT-proces	CobiT-procesdoel en –activiteiten	IdM-aspect
DS1 Define and Manage Service Levels	Doel: definiëren en beheren van service levels opdat een gemeenschappelijk beeld wordt verkregen van de servicevereisten. • Manage service levels • Monitor service levels • Report service levels to customers. Toelichting: Uit de toegang tot programmatuur en gegevens moeten beveiligingseisen worden afgeleid en worden opgenomen in de SLA.	IdM-tools bieden hierbij ondersteuning door bedrijfsprocessen en/of rollen te administreren en hierover te rapporteren. Tevens is vaak een SLA-rapportage mogelijk over de normafwijkingen.
DS2 Manage Third-Party Services	Doel: dit proces vereist dat de rollen en verantwoordelijkheden van derden duidelijk worden gedefinieerd en nagekomen en constant voldoen aan de vereisten. • Organise supplier interface • Report service levels	Dit is een basisfunctionaliteit van een IdM-product.
DS5 Ensure Systems Security	Doel: zekerstellen van systeembeveiliging teneinde de informatie te beveiligen tegen ongeautoriseerd gebruik, openbaarmaking of aanpassing, verminking of verlies. • Define and maintain security measures and procedures • Report security deviations and breaches of the rules and regulations • Monitor the process	Het bewaken van de toegang tot informatie op basis van beveiligingsmaatregelen vereist onder andere toegangscontrole. IdM-oplossingen bieden hiertoe een heel scala van mogelijkheden en ondersteunen en vergemakkelijken het beheer hiervan. Tevens voorzien zij in rapportages met SLA-normafwijkingen.
DS9 Manage the Configuration	Doel: beheer alle ICT-componenten van de ICT-configuratie zodat ongeautoriseerde wijzigingen worden voorkomen, fysieke aanwezigheid wordt geverifieerd en een goede basis wordt geboden voor het change management-proces. • Define and maintain configuration management strategy, policies & procedures	In de praktijk gebruiken niet veel bedrijven de CMDB (Configuration Management DataBase) voor het registreren van beveiligingsniveaus per CI (Configuration Item). Ook is een koppeling tussen de CMDB en de IdM-functies veelal niet gelegd. Door IdM-producten deze functies te laten vervullen is het mogelijk hier integraal invulling aan te geven. Hierbij is een koppeling tussen de CMDB-software en IdM-software een vereiste. Dit bevordert tevens de consistentie van CI's die überhaupt worden geregistreerd i.v.m. authenticatie, autorisatie en provisioning.
DS11 Manage Data	Doel: beheer van data om zeker te stellen dat de data compleet, accuraat en geldig blijven gedurende de input, update en opslag. • Define and implement data processing and controls • Ensure data integrity	Sommige IdM-tools ondersteunen workflow management door het definiëren van policy's, autorisaties, business rules en dergelijke. Hierdoor wordt invulling gegeven aan de vereiste controls.
DS13 Manage Operations	Doel: het beheren van dagelijks beheer om zeker te stellen dat belangrijke IT-supportfuncties regelmatig worden uitgevoerd op een ordelijke manier. • Implement operations procedures and instructions • Report controls for processing and instructions	Procedures voor het toegang verlenen tot o.a. gegevens en het aanmaken van gebruikers. Over de lifecycle van de betrokken gegevens kan worden gerapporteerd. Uiteraard is dit een subset van user access management.

Tabel 2 Relatie tussen CobiT en IdM

CobiT-proces te kijken in hoeverre de activiteiten van dit CobiT-proces worden ondersteund door IdM-functionaliteiten. Hierbij is alleen het CobiT-domein 'Delivery & Support' overgebleven.

Per saldo zijn dus alleen de CobiT-processen DS1, DS2, DS5, DS9, DS11 en DS13 van belang voor IdM, zij het met enige mitsen en maren. Modellen laten zich niet zo eenvoudig aan elkaar relateren als gesuggereerd wordt door de kruisjes in tabel 1. De ene relatie is veel sterker dan de andere. Dit bleek ook bij het detailleren van de relatie tussen de CobiT-processen en de COSO-componenten. Zo zijn in het kader over het COSO-framework achter de COSO-controls de CobiT-processen benoemd. Bij het mappen blijkt echter dat meer relaties mogelijk zijn dan aangegeven in tabel 1. Anderzijds zijn sommige relaties uit tabel 1 lastig terug te vinden in het COSO-model[3]. Dit onderbouwt de stelling van ISACA dat de mapping in tabel 1 niet compleet is en de toepassing afhangt van de inschatting door organisaties van de risico's die zij denken te lopen en de wegingsfactoren die zij daaraan toekennen. Hetzelfde wordt expliciet vermeld in de toepassing van de CobiT-controls. Alleen die controls zijn van belang die een geïdentificeerd risico borgen. In dit kader is het wellicht handig eens te kijken naar de complete mapping van de CobiT-processen op de COSO-aspectgebieden. Deze is te downloaden bij ISACA[5].

De business case

Tabel 2 geeft de relatie weer tussen CobiT-processen en IdM-functies, op basis van de afbakening in tabel 1. Hierbij is gebruikgemaakt van de pocket guide *IT Governance*[6]. De relatie die gelegd is, betreft dan ook een *high level scan*. Bij het leggen van de relatie is gekeken in hoeverre IdM-oplossingen het betrokken CobiT-proces *ondersteunen*. Zo is IdM uiteraard *betrokken* bij het CobiT-proces 'Acquire and Maintain Application Software' (AI2) in de zin van aanschaffen van producten. IdM-oplossingen bieden echter geen inkoopfuncties. Ook bieden IdM-oplossingen een generieke functionaliteit, een gegeven waarmee software policy's rekening moeten houden, bijvoorbeeld door aan applicaties eisen te

CobiT-proces	CobiT-procesdoel en -activiteiten	IdM-aspect
PO2 Define the Information Architecture	Doel: optimaliseer de organisatie van het ontwikkelen en beheren van informatiesystemen om te kunnen voldoen aan de business requirements. • Define access rules for the information classes • Define, implement and maintain security level for each of the data classifications identified above the level 'no protection required'	Afhankelijk van de architectuur en functionaliteit van de IdM-oplossing is ondersteuning op dit vlak mogelijk. Te denken valt aan het invullen van de autorisatiemodule van een workflow management-systeem op basis van een koppeling tussen rollen en gegevensklassen.
PO4 Define the IT Organisation and Relationships	Doel: het creëren van een IT-organisatie die in de juiste IT-services voorziet. • Describe roles, tasks, competences and responsibilities for four levels (IT functions, IT department, IT director, IT steering Committee) • Define responsibilities for physical and logical security	Niet alleen eindgebruikers maar ook beheerders moeten voldoen aan beveiligingsvoorschriften. Veel IT-medewerkers hebben talloze wachtwoorden in hun agenda genoteerd. Het beheer van al deze accounts en wachtwoorden wordt door IdM-oplossingen ondersteund en vereenvoudigd. Het beschrijven van wie waar bij mag komen en wat mag doen kan zeker voor grotere beheerorganisaties prima ondersteund worden door IdM-oplossingen.
DS8 Assist and Advise Customers	Doel: het begeleiden en adviseren van klanten opdat de door de klant geconstateerde problemen worden opgelost. • Registration customer queries • Acceptance of customer queries • Classify customer queries • Solving and recovery	Vaak wordt onderschat hoeveel calls bij een servicedesk gaan over accounts en wachtwoorden. Uit onderzoeken blijkt dit op te kunnen lopen tot 40% van de calls. IdM selfservice kan deze belasting enorm reduceren. Tevens worden de wijzigingen uiteraard gelogd voor securityrapportages. Hiermee wordt dus tevens invulling gegeven aan het registreren (gebruiker), accepteren (IdM-tool) en classificeren (IdM-tool). Solving and recovery kan bijvoorbeeld middels provisioning worden ingevuld. Deze efficiëntie verbetering is overigens een van de doelstellingen van COSO.
M1 Monitor the Processes	Doel: het monitoren van de processen om te verzekeren dat de procesperformancedoelen worden behaald. • Collect monitoring data • Manage reporting for management	Het verzamelen van aan IdM gerelateerde informatie is standaard in de IdM-tools ingebouwd. Tevens bieden de meeste tools uitgebreide rapportagefunctionaliteit om verslagen over de gestelde normen te kunnen genereren. Een voorbeeld hiervan is het aantal selfservice requests in een bepaalde periode ter vermindering van de belasting van de servicedesk.

Tabel 3 Overige relaties tussen CobiT en IdM

stellen ten aanzien van de interface met de IdM-oplossing voor provisioning. Dit betekent echter nog niet dat er daarom een IdM-relatie is onderkend met AI2.

Zoals gesteld is de COSO/CobiT-mapping van ISACA slechts een indicatie. In tabel 3 zijn de overige relaties tussen CobiT en IdM weergegeven.

Conclusie

De brug die COSO en CobiT vormen tussen wet- en regelgeving en beheer levert een duidelijke business case voor IdM als het gaat om SOX en de Code Tabaksblat. IdM is echter geen invulling voor alle vereisten. Er zullen veel meer maatregelen moeten worden getroffen op het gebied van zowel bedrijfsprocessen als beheerprocessen. De mate waarin IdM invulling geeft aan de vereisten is te meten aan de invulling van de CobiT-controls. IdM levert in ieder geval bij zes van de twaalf CobiT-processen waar ISACA de focus op legt, een bijdrage aan het inregelen van CobiT-controls. Tevens zijn er buiten deze twaalf CobiT-processen nog in ieder geval vier andere CobiT-processen die door IdM ondersteund worden. Uiteraard zijn er andere business cases voor het inregelen van IdM-toepassingen denkbaar. Deze vallen echter buiten het bestek van dit artikel.

Drs. ing. Bart de Best RI is werkzaam als service manager bij Qforce B.V.
Met dank aan Willem van Dis, IdM consultant bij ManageID, voor zijn medewerking aan dit artikel.

Noten

1 Looijen, M., *Beheer van informatiesystemen*, ten Hagen en Stam Uitgevers/Sdu Uitgevers, 2004
2 Office of Internal Auditing, Summary of COSO Integrated Framework, december 1999, www.internalauditing.mnscu.edu/projects/CFFOpresentation/COSO1227.pdf
3 Zie noot 2
4 Meetmethode ITIL: www.itsmf.com/bestpractice/selfassessment.asp
5 Complete mapping COSO/CobiT: www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=17901
6 Brand, K. en H. Boonen, *IT Governance: a pocket guide based on COBIT*, Van Haren Publishing, 2004