
Ruben de Wolf

Ervaringen met geïntegreerde IT-controleraamwerken

De kunst van het loslaten

M.C. Wolters RE CISA
is senior manager bij KPMG IT Advisory. Zijn aandachtsgebieden zijn de organisatorische en beheer(s)aspecten van IT, met als focus informatiebeveiliging, outsourcing en projectmanagement. Tevens is hij docent aan de postdoctorale opleidingen Executive Master of IT Auditing en Executive Master of Internal Auditing aan de Universiteit van Amsterdam.

wolters.koos@kpmg.nl

Ir. R. de Wolf RE
is als senior manager werkzaam bij KPMG IT Advisory. Zijn aandachtsgebieden zijn informatiebeveiliging en de robuustheid van omvangrijke, complexe IT-infrastructuren. Hij is trekker van een team van security professionals en docent aan de Universiteit van Amsterdam.

dewolf.ruben@kpmg.nl

P. van Houten MSc
is als junior adviseur werkzaam bij KPMG IT Advisory. Hij voert diverse audit- en adviesopdrachten op het gebied van IT Security en IT Governance uit. Vanuit KPMG is hij als kennismanager betrokken bij de service line Information Protection & Business Resilience.

vanhouten.pieter@kpmg.nl

Koos Wolters RE CISA, ir. Ruben de Wolf RE en Pieter van Houten MSc

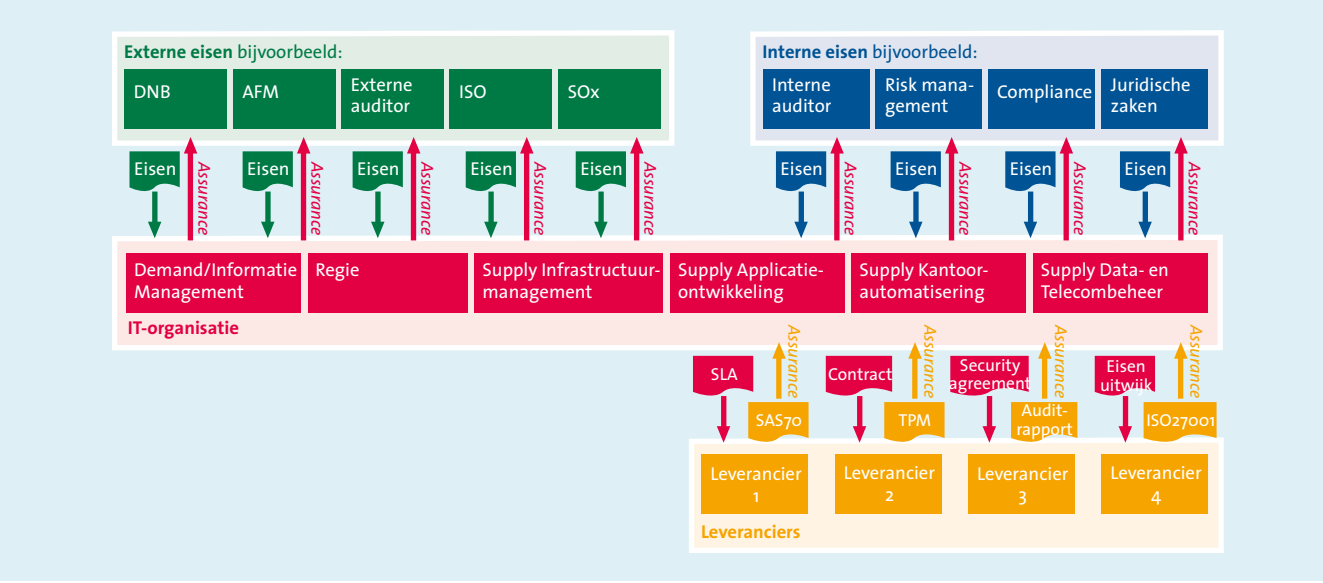
Ondernemingen ervaren een aanzienlijk grotere regeldruk dan vijf à tien jaar geleden, zo ook op het vlak van de beheersing van informatietechnologie. Door wet- en regelgeving en interne richtlijnen op het gebied van bijvoorbeeld informatiebeveiliging, IT compliance, IT General Controls, en operational risk management kost het organisaties veel (dubbel) werk om interne en externe partijen te voorzien van de nodige verantwoordingsinformatie. In de praktijk bestaat een grote overlap tussen de controledoelstellingen of controlemaatregelen waaraan voldaan moet worden. Daarom wordt naarstig gezocht naar één integraal kader voor de beheersing van de IT-omgeving (IT-controleraamwerk) waar CFO's en controllers, CIO's, security managers, risk managers, compliance officers, interne auditors en accountants op kunnen steunen. Dit komt neer op een eenduidig stelsel aan controlemaatregelen waaraan de organisatie moet voldoen en waar zij op haar beurt ook andere partijen aan moet houden. De uitkomsten van twee workshops op het KPMG IT Najaarsevent vormen de basis voor dit artikel over de stand van zaken van en ervaringen met geïntegreerde IT-controleraamwerken.

Inleiding

Regeldruk

De laatste jaren staan ondernemingen onder een toenemende regeldruk. Nationale en internationale wetgeving verplicht ondernemingen inzicht te geven in de kwaliteit van de financiële verantwoording. Voorbeelden zijn de gevolgen van de Sarbanes Oxley[1] (SOx)-wetgeving voor aan Amerikaanse beurzen genoteerde ondernemingen en voor de Nederlandse corporate governance code van de commissie-Tabaksblat[2]. Voor het bank- en verzekeringswezen geldt aanvullende wetgeving zoals de Wet op het financieel toezicht (Wft)[3] en Basel II[4]. Maar ook de overheid staat onder grotere druk om de privacy van

1 Sarbanes-Oxley Act of 2002 – 23 januari 2002.
2 De Nederlandse corporate governance code – Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen – 9 december 2003.
3 Wet houdende regels met betrekking tot de financiële markten en het toezicht daarop – 28 september 2006.
4 Basel Committee on Banking Supervision, Principle 1 – Framework for Internal Control Systems in Banking Organisations – september 1998 en Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards – juni 2006.



Figuur 1. **De controleomgeving van een willekeurige IT-organisatie.**

burgers te waarborgen (Wbp)[5] en om vertrouwelijke en staatsgeheime informatie te classificeren en naar rato te beschermen (VIR-BI)[6].

Deze trend vertaalt zich ook door naar het IT-werkveld. Security managers, compliance officers, risk managers en internal auditors ervaren een wirwar aan overlappende IT-kaders waarover de onderneming dient te rapporteren. Zo rapporteert de CFO over SOx-artikel 404 en functiescheiding, de security manager over ISO 27002[7], de CIO over onder meer IT-dienstverleningsniveaus en de kwaliteit van ITIL-processen, alsook de interne auditor en huisaccountant over General IT Controls en IT-governanceraamwerken zoals COSO[8] en Cobit[9]. De meeste organisaties hanteren hierbij intern ontwikkelde policies, richtlijnen en baselines voor IT-beheer en -beveiliging.

Het gevolg hiervan is dat veel dubbel werk plaatsvindt. Vanwege de diverse, onafhankelijke rapportageverplichtingen worden veel IT controls meervoudig gecontroleerd en gerapporteerd. Het is dan ook niet vreemd dat vrijwel alle grote en middelgrote ondernemingen op zoek zijn naar een efficiëntere manier om verantwoordingsinformatie te verzamelen over het 'in control' zijn van de IT-functie. Niet alleen om dubbel werk te voorkomen, de IT-organisatie te ontlasten en eventueel kosten te besparen, maar ook om tijdiger te kunnen rapporteren. Veel organisaties worstelen namelijk met de periodiciteit en tijdigheid van verantwoordingsrapportages en komen hierdoor in de problemen met hun toezichthouders. Tevens kan door een organisatie op deze manier een gemeenschappelijk kader voor beheersing van de IT-omgeving worden gecreëerd, wat het spreken van gedeelde taal van alle relevante partijen ten aanzien van beheersing en controle van de IT-omgeving doet bevorderen.

De controleomgeving

De controleomgeving van middelgrote en grote ondernemingen bestaat uit een groot aantal in- en externe wet- en regelgevers en andere stakeholders zoals klanten en leveranciers. Deze stakeholders willen via wetten, richtlijnen en contracten invloed uitoefenen op de mate van beheersing van informatietechnologie, temeer als de organisatie sterk afhankelijk is van haar IT voor de betrouwbaarheid en continuïteit van de bedrijfsvoering. Als antwoord op de eisen van de stakeholders dient de IT-organisatie verantwoordingsinformatie te overleggen over de mate waarin is voldaan aan deze eisen. Bij voorkeur wordt deze verantwoordingsinformatie getoetst door een onafhankelijke partij, waardoor meer zekerheid of 'assurance' afgegeven kan worden dat daadwerkelijk aan de eisen is voldaan.

In figuur 1 is een schema opgenomen waarin deze controleomgeving is gevisualiseerd.

Outsourcing als drijfveer tot rationalisatie

Deze behoefte tot rationalisatie van kaders voor de beheersing van IT wordt nog eens versterkt door de trend om de IT te outsourcen. Veel ondernemingen zetten hun IT-beheer- en

5 Wet houdende regels inzake de bescherming van persoonsgegevens – 6 juli 2000.
6 Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie – 1 maart 2004.
7 BS ISO/IEC 27002:2005.
8 Enterprise Risk Management – Integrated Framework – september 2004.
9 Cobit 4.1 – 2007.

-ontwikkelingsactiviteiten buiten de deur. IT-dienstverleners streven naar verregaande standaardisatie van hun IT-dienstverlening en hebben hun werkprocessen doorgaans ingericht volgens open standaarden of 'good practice guidelines'. Daarnaast leidt het uitbesteden van IT volgens de richtlijnen en baselines van de opdrachtgever tot maatwerk voor de IT-dienstverlener en daarmee tot hogere kosten. Ook dit is voor ondernemingen een extra drijfveer om zowel intern als richting IT-dienstverleners met één IT-controleraamwerk op basis van open standaarden te werken.

Wanneer bijvoorbeeld het beheer van (delen van) een IT-omgeving is uitbesteed, is het gebruikelijk dat over deze dienstverlening een assuranceverklaring (SAS 70, TPM of anderzijds) wordt verkregen van een externe auditor. Deze auditor wordt meestal aangewezen door de leverancier. In het geval van financiële dienstverleners of banken is dit zelfs door toepasselijke wet- en regelgeving noodzakelijk.

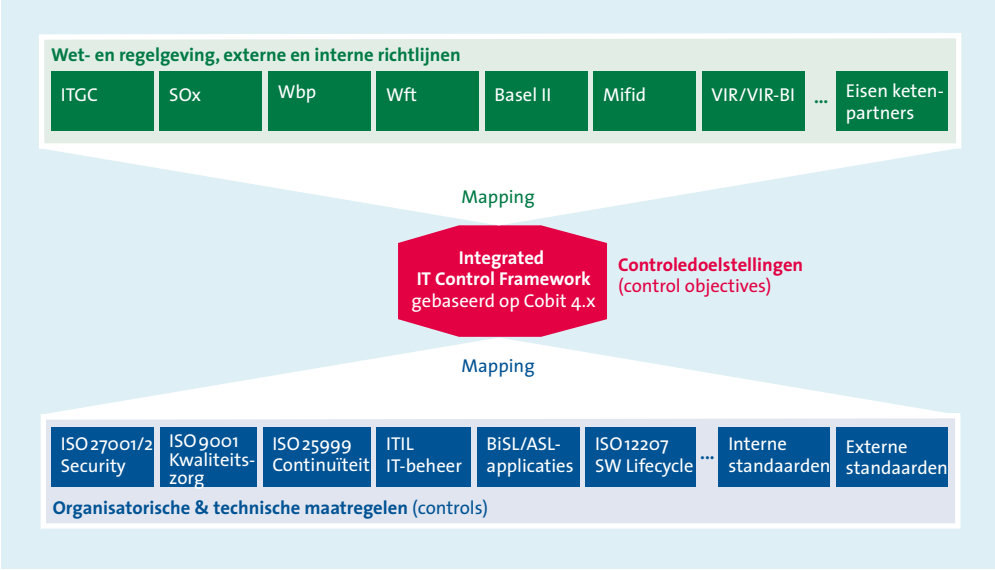
Ook in dergelijke gevallen kan een IT-controleraamwerk dienst doen als referentiekader voor de eisen die de organisatie stelt aan de beheersing van haar IT-omgeving. Het IT-controleraamwerk moet dan wel zijn opgenomen als onderdeel van het contract tussen de uitbestedende organisatie en haar leverancier. De externe auditor die een assuranceverklaring afgeeft, zal in de praktijk in overleg met zijn opdrachtgever een selectie maken van de controls in het IT-controleraamwerk die als relevant worden beschouwd voor de uitbestede IT-diensten.

Basisprincipes geïntegreerde IT-controleraamwerken

Structuur

Een geïntegreerd IT-controleraamwerk is een kader waarin alle relevante IT-richtlijnen zijn gekoppeld aan universele controledoelstellingen. Tevens kunnen deze controledoelstellingen gekoppeld zijn aan of verder uitgewerkt zijn in controlemaatregelen of controls. Het merendeel van de organisaties die bezig zijn met een integraal framework, hanteert Cobit 4.x als 'kapstok' en zoekt naar manieren om vanuit de controledoelstellingen die in Cobit[10] zijn opgenomen relaties te leggen met de diverse interne en externe regelgeving.

In figuur 2 is de structuur van een geïntegreerd IT-controleraamwerk schematisch weergegeven. Vanuit de diverse interne en externe wetten, regelgeving en richtlijnen wordt een koppeling of 'mapping' gemaakt naar relevante gedetailleerde controledoelstellingen uit Cobit. Op dat moment zijn de diverse eisen uit de wet- en regelgeving dus verzameld in één eenduidige set van controledoelstellingen.



Figuur 2. **Structuur integraal IT-controleraamwerk.**

Volledig en herbruikbaar

Onze ervaring leert dat veel organisaties steunen op een selectie van Cobit controls die door de organisatie van belang wordt geacht. Zelden wordt een integraal control framework opgebouwd aan de basis: de verschillende wet- en regelgeving waar de noodzaak van het framework mee begon. Indien organisaties daadwerkelijk inzichtelijk willen krijgen welke beheersingsdoelstellingen gehaald dienen te worden vanuit specifieke wet- en regelgeving, zal een mapping gemaakt moeten worden van deze wet- en regelgeving naar (bijvoorbeeld) de Cobit-controledoelstellingen (control objectives).

De koppelingen van relevante wet- en regelgeving voor een specifieke branche naar controledoelstellingen kunnen voor alle

10 Cobit bestaat uit een deming cycle van Plan and Organise, Acquire and Implement, Deliver and Support, en Monitor and Control. Deze hoofdonderdelen vallen uiteen in diverse high level control objectives (zoals bijvoorbeeld Manage Changes of Ensure System Security). Deze high level control objectives zijn op hun beurt weer onderverdeeld in detailed control objectives.

organisaties in die branche worden gebruikt. Daarnaast wordt met het gebruik van Cobit als model voor de controledoelstellingen een algemene standaard geïntroduceerd die breed is geaccepteerd. Hoewel herbruikbaar dient het raamwerk te allen tijde afgestemd te worden met en goedgekeurd te worden door de betrokken functionarissen binnen en buiten de organisatie, zoals de externe accountant.

De kracht zit 'm niet in de details

Aangezien een aantal wet- en regelgevers zeer gedetailleerde eisen stelt aan de IT-organisatie is het soms noodzakelijk om deze controledoelstellingen nog nader uit te werken. Daarvoor worden algemeen geaccepteerde specifieke maatregelensets (zoals ISO-normen en andere standaarden) gebruikt. Ook dan vindt een koppeling plaats van de gedetailleerde controledoelstellingen van Cobit naar deze specifieke maatregelen of controls. Zie ook de onderzijde van figuur 2.

De kracht van een geïntegreerd IT-controleraamwerk wordt vooral bereikt wanneer deze op het niveau van gedetailleerde controledoelstellingen van Cobit is uitgewerkt en de diverse betrokken partijen, zoals IT-dienstverleners, de vrijheid behouden om zelf een keuze te maken voor de invulling van specifieke maatregelen, mits de controledoelstellingen maar worden gehaald.

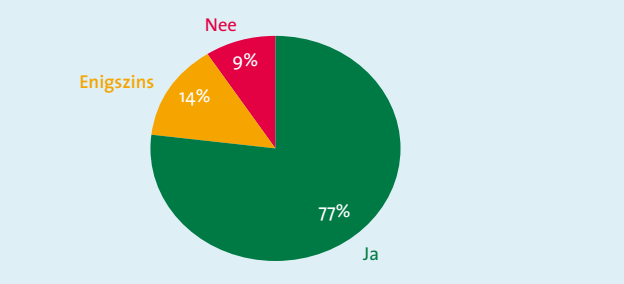
Uitkomsten workshop: waar staan organisaties nu?

Workshops

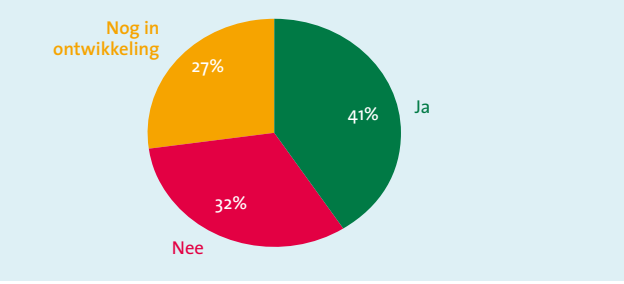
Tijdens het KPMG IT Najaarsevent hebben de auteurs een tweetal workshops gehouden met in totaal circa veertig deelnemers. De deelnemers waren afkomstig uit een diversiteit aan organisaties (banken, verzekeringsmaatschappijen, industriële ondernemingen, overheidsinstanties, IT-serviceproviders) en hadden zeer verschillende functies (CIO, CFO, hoofden risk management, hoofden internal audit). In deze workshops is de deelnemers met behulp van een interactief stemsysteem een aantal vragen gesteld over drijfveren, de stand van zaken en verwachte merites van geïntegreerde IT-controleraamwerken.

Hieronder volgt een samenvatting van de belangrijkste resultaten van de workshops:

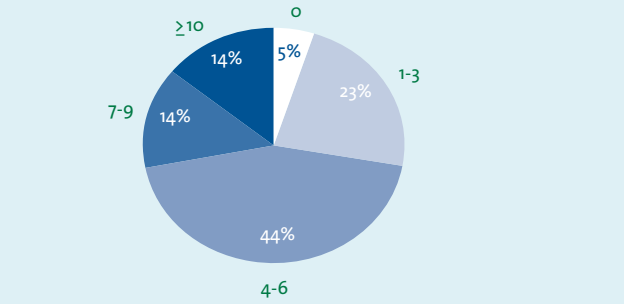
- Meer dan driekwart van de deelnemers ziet voordelen bij de implementatie van een geïntegreerd IT-controleraamwerk (figuur 3).
- Uit de workshops bleek dat zestig procent van de deelnemende organisaties nog geen geïntegreerd IT-controleraamwerk heeft of bezig is om dit te ontwikkelen. De overige veertig procent gaf aan al te beschikken over een dergelijk raamwerk (figuur 4).



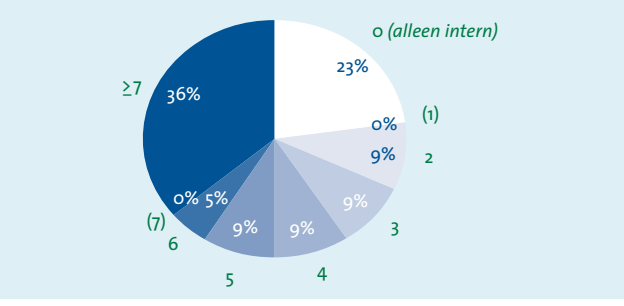
Figuur 3. **Zien de deelnemers voordelen bij de implementatie van een integraal IT-controleraamwerk?**



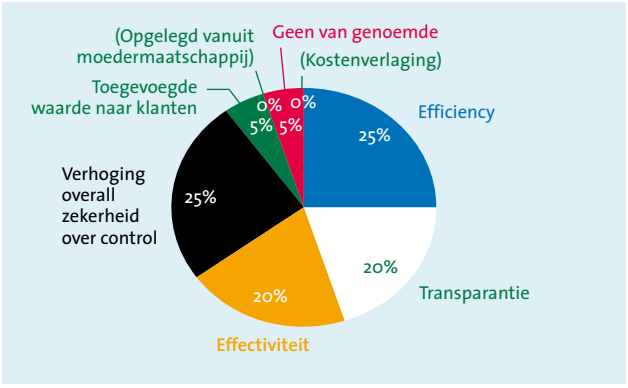
Figuur 4. **Hebben de organisaties van de deelnemers reeds een geïntegreerd IT-controleraamwerk?**



Figuur 5. **Aan hoeveel verschillende typen wet- en regelgeving moeten de organisaties van de deelnemers naar schatting voldoen?**



Figuur 6. **Op hoeveel IT-dienstverleners steunt de organisatie voor beheer, ontwikkeling en onderhoud van IT?**



Figuur 7. **Belangrijkste drijfveer voor de organisatie om een integraal IT-controleraamwerk in te richten?**

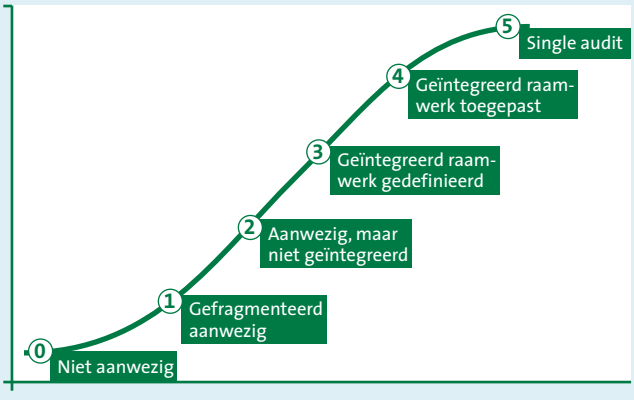
- Driekwart van de deelnemers gaf aan te moeten voldoen aan meer dan vier verschillende typen wet- en regelgeving op het vlak van IT-beheersing. Een kwart gaf zelfs aan te maken te hebben met meer dan zeven verschillende typen wet- en regelgeving op dit vlak (figuur 5).
- Hetzelfde bleek het geval te zijn voor het aantal externe en interne partijen waaraan de IT-organisaties van de aanwezigen verantwoording dienen af te leggen. Driekwart legt aan meer dan vier verschillende partijen verantwoording af over de beheersing van IT.
- Tweederde van de deelnemers geeft aan te steunen op meer dan drie IT-dienstverleners voor beheer, onderhoud en/of ontwikkeling van IT. De helft daarvan heeft zelfs meer dan zeven IT-dienstverleners (figuur 6).
- Tweederde van de deelnemers geeft aan de assurance-informatie die IT-dienstverleners aanleveren niet direct of in het geheel niet te kunnen relateren aan de voor de organisatie relevante wet- en regelgeving. Dit wil zeggen dat in tweederde van de gevallen nog een vertaalslag nodig is ter verantwoording aan de stakeholders van de betreffende organisaties.
- Geen van de aanwezigen ziet hierbij kostenverlaging als belangrijkste drijfveer. Als eerste worden genoemd 'efficiencyverhoging' en 'overall zekerheid over IT-controle' en vervolgens 'verbeteren van transparantie' en 'verbeteren effectiviteit van IT-controle' (figuur 7).
- Alle aanwezigen verwachten dat het implementeren van een geïntegreerd IT-controleraamwerk een meerjarentraject is.

Volwassenheidsmodel

Om een beeld te geven van waar organisaties staan in de ontwikkeling van geïntegreerde IT-controleraamwerken, hebben de auteurs een volwassenheidsmodel opgesteld. In figuur 8 is dit model grafisch weergegeven.

In tabel 1 zijn de vijf niveaus nader toegelicht.

Net als bij de meeste volwassenheidsmodellen betreft niveau 5 'Single audit' hier een niveau waarnaar gestreefd kan worden, maar wat uiteindelijk voor veel organisaties slechts een ijkpunt zal zijn dat in de nabije toekomst niet snel zal worden gehaald. Uit de workshops bleek dat vrijwel alle deelnemers zich op niveau 0 tot en met 3 bevinden. Drie deelnemers (nog geen tien procent) schatten in dat zij op niveau 4 actief zijn. Geen van de deelnemers bevindt zich op niveau 5.



Figuur 8. **Volwassenheidsmodel geïntegreerde IT-controleraamwerken.**

Nr.	Niveau	Toelichting
0	**Niet aanwezig**	• Geen gebruik van kaders inzake beheersing IT
1	**Gefragmenteerd aanwezig**	• Kaders voor IT-beheersing gefragmenteerd aanwezig • Overall structuur en koppeling met diverse interne en externe wet- en regelgeving ontbreekt
2	**Aanwezig maar niet geïntegreerd**	• Verschillende kaders voor IT-beheersing aanwezig en koppeling met diverse interne en externe wet- en regelgeving gemaakt • Diverse kaders niet geïntegreerd
3	**Geïntegreerd aanwezig**	• Gedefinieerd proces waarin alle bestaande IT-kaders zijn gebaseerd op diverse interne en externe wet- en regelgeving • IT-kaders volledig geïntegreerd op niveau van controledoelstellingen
4	**Geïntegreerd in gebruik als toetsingsinstrument**	• Diverse partijen gebruiken raamwerk • Geen steun op door anderen getoetste controledoelstellingen
5	**Single audit**	• Elke controledoelstelling uit raamwerk enkelvoudig getoetst en meervoudig gebruikt • Partijen steunen dus op controlewerkzaamheden van andere partijen

Tabel 1. **Volwassenheidsmodel voor het hanteren van geïntegreerde IT-controleraamwerken.**

Praktijkervaringen

Het opzetten van een geïntegreerd IT-controleraamwerk zoals hiervoor geschetst is geen sinecure. Het vergt de nodige ervaring met de betreffende wet- en regelgeving en ook met de ins en outs van modellen zoals Cobit. De diverse wet- en regelgeving geeft veel ruimte voor interpretatie. Ook de betrokken partijen hebben vanuit hun eigen achtergrond een eigen voorkeur voor de interpretatie van deze wet- en regelgeving en de wijze van koppeling van de wet- en regelgeving aan de Cobit controls.

Vaststellen raamwerk

De belangrijkste uitdagingen bij het *vaststellen* van een geïntegreerd IT-controleraamwerk zijn:

- het vaststellen welke regelgeving allemaal voor de organisatie van toepassing is én relevant is voor de IT-omgeving;
- de specifieke vertaling van eisen vanuit de wet- en regelgeving naar eisen voor de IT-omgeving van de organisatie;
- het verkrijgen van overeenstemming over de inhoud van het raamwerk en de diepgang waarmee het raamwerk wordt opgezet;
- het interpretatieloos vastleggen van de controles in het IT-controleraamwerk;
- het overtuigen van de betrokken partijen dat door één uniform IT-controleraamwerk in te voeren en te steunen op de controles van anderen, de mate van beheersing van de IT-omgeving niet minder wordt.

In figuur 9 is een voorbeeld gegeven van de vastlegging van een IT-controleraamwerk zoals dat voor een organisatie in de financiële sector is vormgegeven.

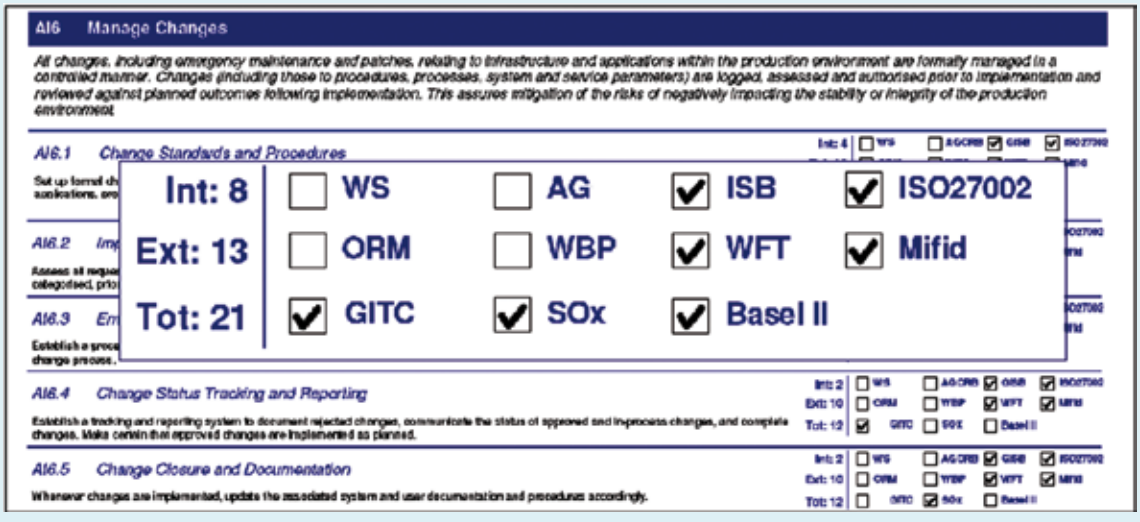
In deze figuur is voor het onderdeel AI6.1 Manage Changes / Change Standards and Procedures uit Cobit 4.1 te zien aan welke in- en externe wet- en regelgeving deze gedetailleerde controledoelstelling is gekoppeld. Daarnaast is een duidelijk onderscheid gemaakt tussen het aantal keren dat de control is gekoppeld aan interne en externe wet- en regelgeving. Ook is aangegeven hoe vaak de control in totaal is gekoppeld. Deze statistische informatie kan belangrijke uitgangspunten bieden bij het bepalen van het belang van een bepaalde controledoelstelling. Het mag duidelijk zijn dat de mate waarin de interne en externe wet- en regelgeving gekoppeld is aan een controledoelstelling, indiceert in hoeverre de controledoelstelling een belangrijke bijdrage levert aan de beheersing van de IT-omgeving van de organisatie.

In figuur 10 is als voorbeeld een gedeelte van een koppeling van ISO 27001 naar Cobit 4.1 weergegeven.

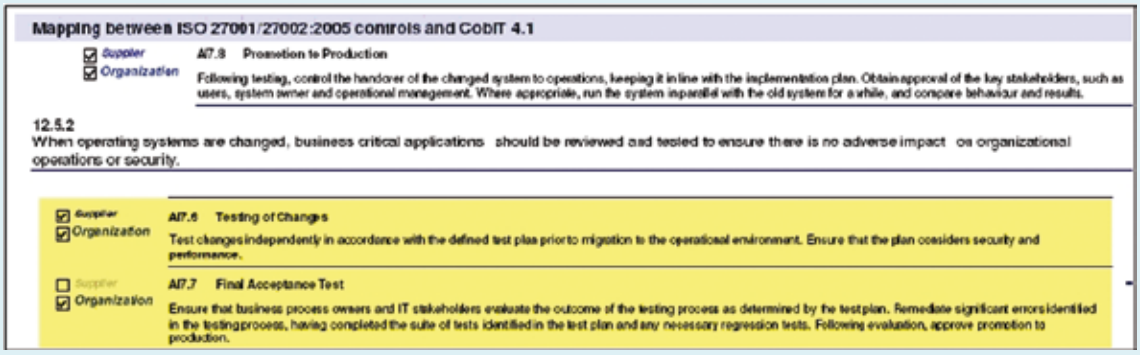
Gebruik raamwerk

In onze ervaring is het opzetten en vastleggen van het raamwerk echter niet het moeilijkste onderdeel van de implementatie. Wanneer het raamwerk uiteindelijk is vastgelegd, is de grootste hobbel die nog genomen moet worden, het daadwerkelijk in gebruik nemen van het framework.

De lijn- en IT-organisatie dienen de juiste controls te selecteren bij de controledoelstellingen en deze door te voeren in IT-processen en -procedures. Waar nodig dienen interne controles te worden uitgevoerd op de juiste werking van deze controls. De controlerende stafafdelingen en externe toezichthouders, in het bijzonder de externe accountant, dienen op basis van dit model reviews, controles en audits uit te voeren. In geval van uitbe-



Figuur 9. **Voorbeeld van een IT-controleraamwerk.**



Figuur 10. **Voorbeeldmapping ISO 27001.**

steding van de IT-dienstverlening dient een deel van deze controls te worden overgedragen aan IT-dienstverleners, wat wil zeggen dat gesteund moet worden op verantwoordingsinformatie die door de IT-dienstverlener wordt verstrekt, bijvoorbeeld in de vorm van een TPM of SAS 70-verklaring.

De belangrijkste uitdagingen bij het *implementeren* van een geïntegreerd IT-controleraamwerk zijn:

- het maken van duidelijke afspraken over de wijze waarop invulling wordt gegeven aan het IT-controleraamwerk. Wie gaan met het raamwerk werken en op welke manier?
- het bepalen van de manier waarop toetsing door de controlerende instanties (intern en extern) plaatsvindt. Is dit op basis van de controledoelstellingen of dient het raamwerk nog te worden uitgebreid naar meer gedetailleerde controles?
- het bepalen van de manier waarop het raamwerk aan mogelijke externe partijen wordt gecommuniceerd.
- het zorgen voor eigenaarschap van het IT-controleraamwerk, maar ook voor eigenaarschap van de koppelingen met wet- en regelgeving, zodat wijzigingen in wet- en regelgeving ook worden doorgevoerd in het raamwerk.

Aan het einde van dit artikel zijn de belangrijkste succesfactoren voor het implementeren van een geïntegreerd IT-controleraamwerk kort samengevat.

Ruben de Wolf geeft een nadere toelichting over het IT-controleraamwerk tijdens de terugkoppelingssessie.

Conclusies

Een goed functionerend geïntegreerd IT-controleraamwerk kan een zegen zijn voor een organisatie die gebukt gaat onder de zoveelste auditor, externe toezichthouder of certificerende instantie die langskomt om voor de zoveelste keer in hetzelfde jaar dezelfde vragen te stellen aan net die ene medewerker die al overladen is met werk. Met de juiste expertise en middelen, de juiste mindset bij de stakeholders en de bereidheid van partijen om te steunen op het werk van anderen kan een dergelijk raamwerk voor werklastverlichting zorgen.

Daarnaast heeft een dergelijk raamwerk ook nog andere voordelen, zoals:

- transparantie (in- en extern één taal spreken ten aanzien van beheersing);
- effectiviteit (voorkomen van blinde vlekken in de aanpak);
- kostenverlaging;
- verhogen van de overall zekerheid over de beheersing van de IT-omgeving;
- toegevoegde waarde naar klanten.

Vooral organisaties die te maken hebben met een groot aantal verschillende toezichthouders en met diverse typen wet- en regelgeving op het vlak van IT-beheersing en die met meerdere IT-dienstverleners zaken doen, kunnen baat hebben bij een dergelijk raamwerk.

Het succes van de invoering van een geïntegreerd IT-controleraamwerk is zowel afhankelijk van de intrinsieke kwaliteit van het raamwerk, als van de mate waarin de betrokken partijen bereid zijn om het raamwerk te adopteren en te steunen op elkaars controleresultaten. In de kern komt dit neer op een deel van de eigen IT-controlewerkzaamheden durven loslaten. Hierin dient ons inziens de externe IT-auditor een voortrekkersrol te vervullen. Niet alleen beschikt deze over een gedegen kennis van relevante wet- en regelgeving en passende controleraamwerken, ook is de externe IT-auditor één van de belangrijkste spelers die moet durven loslaten en zijn controleaanpak meer systeemgericht dient in te richten.

Belangrijkste succesfactoren voor de implementatie van een geïntegreerd IT-controleraamwerk:

- Betrek alle partijen direct vanaf het begin bij de totstandkoming van het raamwerk.
- Neem voldoende tijd voor de uitwerking van het raamwerk, net als bij zoveel zaken is ook in dit geval haastige spoed zelden goed.
- Stel duidelijk vast welke partijen stakeholder zijn en neem al deze partijen stap voor stap mee in de totstandkoming van het raamwerk.
- Maak gebruik van interne of externe expertise op het gebied van het te gebruiken IT-controleraamwerk (bijvoorbeeld Cobit), de te koppelen interne en externe wet- en regelgeving en de meer gedetailleerde standaarden met concrete maatregelen en procedures.
- Formuleer de reikwijdte van het raamwerk en communiceer dit aan de stakeholders.
- Tracht een zo integraal mogelijk model vast te stellen.
- Borg een actieve bijdrage vanuit de verschillende disciplines binnen de (lijn)organisatie.
- Zorg voor een werkbare tool waarin de koppeling tussen de verschillende interne en externe wet- en regelgeving goed kan worden geadministreerd.
- Gebruik voor deze koppeling één integraal raamwerk zoals Cobit.
- Zorg voor een zorgvuldig en geformaliseerd afstemmingsproces.
- Beleg het eigenaarschap van het totale IT-controleraamwerk.
- Maak afspraken over de wijze waarop na vaststelling met het raamwerk zal worden gewerkt.
- Maak zoveel mogelijk gebruik van algemeen geaccepteerde koppelingen tussen de verschillende standaarden en wet- en regelgeving, bijvoorbeeld van ISACA (zij heeft diverse standaardmappings van wet- en regelgeving naar Cobit).