SAS 70 als alternatief voor ISO 9001-certificatie

GENERIEK OF MAATWERK

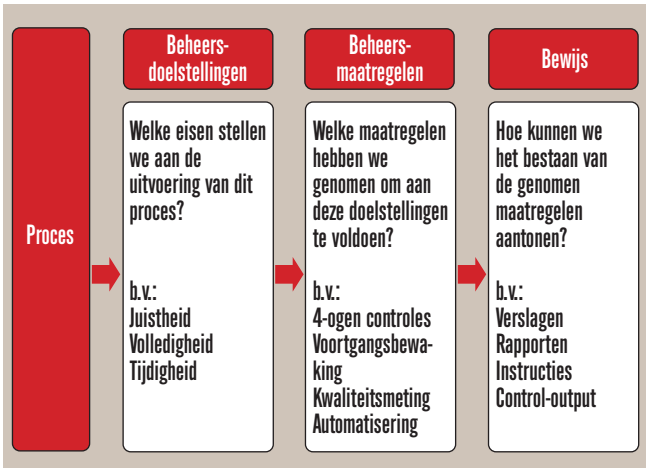
Dit artikel beschrijft de praktijk bij een grote pensioenverstrekker waar zowel ISO 9001 als ook SAS 70 tot het werkveld behoren, en geeft uitleg over de achtergrond en toepassing van SAS 70 aan de hand van voorbeelden binnen deze organisatie. SAS 70 en ISO 9001 worden vergeleken wat betreft inhoud en toepassingsmogelijkheden. Centraal staat de vraag: kan SAS 70 als alternatief fungeren voor ISO 9001-certificatie?

Door Robert Klingens

ISO 9001-certificatie is nog steeds uiterst actueel als manier om aan klanten kwaliteitsbeheersing aantoonbaar te maken. Nederland staat zelfs als tiende in de wereldtop-tien voor wat betreft aantallen ISO 9001-certificaten. Een volledige bedrijfstak van accreditatie- en certificatie-instellingen is dagelijks in de weer om bedrijven te adviseren en te trainen, audits uit te voeren, en te certificeren. Dit ondanks regelmatig terugkerende discussies over toegevoegde waarde en zeggingskracht van het ISO-certificaat.
Vanuit de accountancy is de laatste jaren in het voetspoor van Sarbanes-Oxley een andere methodiek om kwaliteit van dienstverlening inzichtelijk te maken naar voren gekomen: de 'Statement on Auditing Standards No.70', kortweg SAS 70 genoemd. Dit is een Amerikaanse auditingstandaard voor het documenteren van het stelsel van interne beheersmaatregelen ten aanzien van uitbestede processen, het auditen van deze maatregelen op hun toereikendheid en, naar keuze, de werking van de maatregelen. Oorspronkelijk was SAS 70 exclusief gekoppeld aan de jaarrekeningcontrole, er is de laatste jaren echter een trend zichtbaar waarbij een SAS 70 rapport wordt gebruikt als verantwoording over de operationele beheersing (niet of slechts beperkt gekoppeld aan de jaarrekening), of als kwaliteitscertificaat.
Achtergrond en toepassing van het ISO-certificaat worden in dit artikel minder uitgebreid behandeld. Meerdere artikelen in Business Process Magazine hebben hieraan de afgelopen jaren aandacht besteed en kennis hiervan wordt als bekend verondersteld.

Achtergrond en toepassing SAS 70

Het SAS 70 rapport vindt zijn oorsprong in de jaarrekeningcontrole: Het is oorspronkelijk een communicatiemiddel tussen externe accountants van service-organisatie en gebruikersorganisatie onderling in een situatie van uitbesteding. De service-organisatie beschrijft in een rapport op hoofdlijnen de beheerorganisatie en geeft hierbij aan hoe zij specifieke beheersdoelstellingen bereikt. Dit rapport moet worden opgesteld conform de richtlijnen van SAS 70.
Vanuit verschillende invalshoeken wordt van de service-organisatie deze verantwoording vereist:



Afbeelding 1: SAS 70 proces.

- Wanneer het uitbestede proces is gekoppeld aan materiële posten van de jaarrekening, heeft de accountant voor de jaarrekeningcontrole van de gebruikersorganisatie inzicht nodig in de kwaliteit van de procesbeheersing bij de service-organisatie;
- Vanuit Sarbanes-Oxley heeft de gebruikersorganisatie inzicht nodig in de kwaliteit van de procesbeheersing bij de service-organisatie;
- Financiële instellingen bijvoorbeeld hebben te maken met eisen vanuit Basel II, en specifieke eisen vanuit toezicht-houders. Ook voor de door hen uitbestede processen gelden deze eisen.

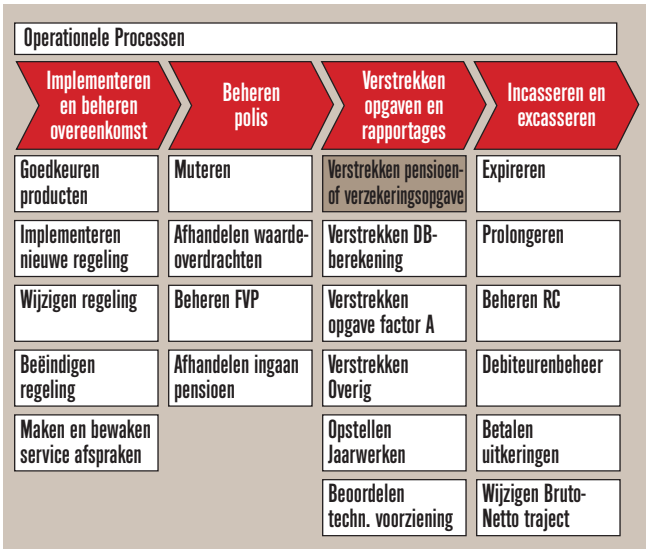
In tegenstelling tot ISO 9001 biedt SAS 70 geen normenkader, maar een set van voorschriften voor de rapportage, waar-binnen de opsteller zelf zijn normenset en beheersmaat-regelen kiest. De opsteller, de service-organisatie, bepaalt in samenwerking met de gebruikersorganisatie, de opdracht-gever, voor welke doelstellingen het SAS 70 rapport wordt opgesteld.

Een SAS 70 traject kan in grofweg vijf stappen worden onderverdeeld.

- *Scoping.* De opdrachtgever (gebruikersorganisatie) vraagt aan de service-organisatie of deze een verklaring kan overleggen voor de processen die de bedrijfsvoering van zijn organisatie beïnvloeden. Hij bepaalt hiermee de scope van de rapportage, inclusief het type verklaring dat nodig is.
- *Beschrijven van beheersdoelstellingen en procesinrichting.* De organisatie dient te worden beschreven en de beheers-maatregelen op organisatorisch niveau, de processen van de service-organisatie en de beheersdoelstellingen. Het COSO-framework wordt hierbij dan vaak als referentie gehanteerd.
- *Toetsen van inrichting en opzet.* Aan de hand van de opge-stelde procesbeschrijvingen en uitgevoerde risico-analyses toetst een externe auditor – vaak een certificerend accoun-tant – de opzet van de processen en systemen. De auditor geeft een verklaring af over de mate waarin de opzet overeenkomt met de beschrijving en of de service-organisatie de beschreven doelstellingen kan bereiken. Dit alles wordt vastgelegd in een SAS 70 Type 1-verklaring.
- *Toetsen van de werking.* Aanvullend kan een service-organisatie ook de werking van de processen en systemen laten auditen. De externe auditor geeft in dat geval een beoordeling over de werking over een periode van mini-maal zes maanden. De processen en systemen worden uitgebreid door de organisatie getest en moeten bewijzen dat ze voldoen aan de beschrijving van de beheerssituatie, zodat de beheersdoelstellingen gehaald kunnen worden. Als de service-organisatie naar behoren functioneert, ontvangt deze een SAS 70 Type 2-verklaring.
- *Beheer.* De SAS 70 verklaring geldt voor één jaar. Daarom moet de lijnorganisatie het beheer efficiënt inrichten om zodoende de continuïteit van de verklaring niet in gevaar te brengen. Dit betekent het actueel houden van de beschrij-vingen en het regelmatig auditen en monitoren van de beheersstructuur.

SAS 70 bij een pensioenverstrekker

De Nederlandsche Bank heeft in de beleidsregel 'Uitbesteding Pensioenfondsen' vastgesteld dat pensioenfondsen die de administratie uitbesteden aan een uitvoerder, voldoende zekerheid dienen te krijgen over het handhaven van een beheerste en integere bedrijfsvoering. Daarnaast willen ook werkgevers zekerheid krijgen over de beheersing van de bedrijfsvoering van de pensioenadministratie.
Dit én directe vragen vanuit de pensioenfondsen waren voor de pensioenverstrekker aanleiding om voor haar werkgever-relaties en pensioenfondsen een SAS 70 Type I-rapport op te stellen. De scope die gebruikt is voor dit rapport is: alle klantprocessen vanaf het implementeren van nieuwe



Afbeelding 2: Schematisch overzicht van alle klantprocessen.

Verstrekken opgaven en rapportages	Verstrekken pensioen- of verzekeringsopgave
Beheersdoelstelling: Uitgevoerde beheersingsmaatregelen bieden in redelijke mate zekerheid dat alle aan de klant/deelnemer ad hoc verstrekte verzekeringsopgaven juist, tijdig en volledig verwerkt worden.	
Het verstrekken van pensioen- of verzekeringsopgaven aan deelnemers.	
Beheersingsmaatregelen	**Commentaar auditor**
De systemen 1 en 2 vervaardigen automatisch pensioen- en verzekeringsopgaven. Een eerste medewerker Services (maker) voert de mutatiedatum en het polisnummer in in systeem 3. Een tweede medewerker Services (controleur) beoordeelt de mutatie op juistheid, correctheid aan de hand van het polisnummer en de mutatiedatum. Zodra de opgave is afgeleverd op de afdeling wordt deze verstuurd naar de desbetreffende klant/deelnemer. De behandelaar c.q. interne account manager (IAM) van het pensioencontract bewaakt initieel via het overzicht openstaande opdrachten in systeem 3 en de stoplichtrapportage de tijdigheid en volledigheid van de ad hoc te verstrekken verzekeringsopgaven. Daarnaast bewaakt de teammanager de tijdigheid en volledigheid aan de hand van de stoplichtrapportage.	Opzet en bestaan vastgesteld. Geen bijzonderheden waargenomen.

Afbeelding 3: Beheersmaatregelen.

pensioencontracten tot en met het beëindigen van bestaande pensioencontracten, inclusief de financiële verantwoording. Zie afbeelding 2.
Het rapport is opgebouwd uit drie secties. De eerste sectie is het Assurance rapport van de externe accountant. Deze sectie bevat de verklaring van de externe accountant omtrent de opzet en inrichting van de beheersmaatregelen. De tweede sectie is de beschrijving van de beheersstructuur. Deze sectie bevat het bedrijfsprofiel van de organisatie, de scope van de werkzaamheden waarover gerapporteerd wordt en de beheersstructuur rondom de processen. De beheersstructuur wordt beschreven aan de hand van een aantal onderdelen van het COSO Enterprise Risk Management Model: Internal Environment, Risk Assessment, Control Activities, Information & Communication en Monitoring.
De derde sectie betreft getroffen beheersingsmaatregelen. Deze sectie bevat alle beheersmaatregelen per proces, aangevuld met de IT General Controls, de beheersmaatregelen om te waarborgen dat de geautomatiseerde systemen input omzetten naar de juiste output. Verder worden de werkzaamheden van de externe accountant beschreven en wordt aangegeven per beheersingsmaatregel wat de bevindingen van de accountant zijn. Afbeelding 3 toont hoe de beheersmaatregelen in het rapport worden gepresenteerd.

Lessons Learned

Gedurende de maanden dat de organisatie aan het SAS 70 traject heeft besteed, is een aantal zaken naar voren gekomen dat doorlooptijd, efficiency en effectiviteit bij vergelijkbare trajecten enorm zou kunnen vergroten:

- Zorg voor een stuurgroep bestaande uit directieleden. Dit waarborgt een soepele doorloop van het project, aangezien operationele en logistieke knelpunten meteen geadresseerd en opgelost kunnen worden;
- Maak vooraf hele heldere afspraken met de externe accountant over verantwoordelijkheden, aanpak, taken en planning, en bewaak deze nauwgezet. Hiermee wordt voorkomen dat er werk dubbel wordt gedaan, of dat er langs elkaar heen wordt gewerkt;
- Zorg ervoor dat het SAS 70 controle-team bestaat uit medewerkers met operationele werkervaring en gedegen kennis van systemen. Nog beter: integreer de kwaliteitsafdeling in het project, zodat gevonden knelpunten meteen in de verbetercyclus meegenomen kunnen worden;
- Begin tijdig met het schrijven van het rapport en zorg dat je vooraf overeenstemming hebt met de externe accountant over de opzet en structuur van de rapportage.

Ook heeft het traject onverwachte positieve effecten opgeleverd die niet waren ingecalculeerd maar dankbaar zijn ontvangen:

- Forse toename van kennis van systemen en processen en hun consequenties voor effectiviteit en efficiency van operations, en financiële verantwoording. De complexiteit is in feite transparanter en inzichtelijk gemaakt;
- Door het toetsen van de beheersingsmaatregelen is er meer aandacht voor die beheersingsmaatregelen in de lijn. De noodzaak om risico management invulling te geven wordt beter begrepen en geaccepteerd;
- Verbeterde samenwerking tussen financiële afdeling, IT-afdeling en de lijnorganisatie, vanwege inzicht in de wederzijdse afhankelijkheden. Door het traject hebben personen en functies elkaar beter leren kennen en spreken elkaar nu sneller aan in het geval van problemen;
- Het rapport is ook zeer nuttig bij het inwerken van nieuwe managers en medewerkers. Er wordt op een simpele en overzichtelijke manier inzicht gegeven in de processen en de beheersstructuur van de organisatie.

Afweging

De vraag aan het begin van dit artikel was: kan SAS 70 als alternatief fungeren voor ISO 9001-certificatie? Om op deze vraag antwoord te geven zullen er eerst drie subvragen gesteld en beantwoord worden: biedt SAS 70 de voordelen van het ISO-certificaat; biedt SAS 70 een oplossing voor de nadelen van het ISO-certificaat en als laatste vraag; biedt SAS 70 nog aanvullende voordelen boven ISO-certificatie? De tabel in afbeelding 5 geeft een uitwerking van de eerste twee vragen.

Biedt SAS 70 nog aanvullende voordelen?

Er is sprake van een grote overlap tussen werkzaamheden voor Sarbanes-Oxley en SAS 70. Hierdoor zou een organisatie die SOX compliant dient te zijn, met SAS 70 met minder inspanning haar procesbeheersing inzichtelijk kunnen maken dan met ISO 9001-certificatie.
Waar ISO-certificatie stopt bij processen, procedures en periodieke kwaliteitsregistraties, duikt SAS 70 de diepte in door *alle* beheersdoelstellingen en beheersmaatregelen per proces in kaart te brengen en volgens een met de externe accountant afgesproken steekproefmethodiek zes maanden tot een jaar (!) te testen. SAS 70 biedt dus gedetailleerder en praktischer inzicht in de processen van de service-organisatie (Meten = Weten).
Het verstrekken van een ISO-certificaat gebeurt meestal op basis van een handboekbeoordeling en een audit van een aantal dagen door de certificerende instelling. In feite wordt het certificaat dus verstrekt op basis van een momentopname. Het oordeel van de externe accountant in een SAS 70 rapport is gebaseerd op minimaal zes maanden testen, onder nauwe

Onderwerp	SAS 70 Type 2	ISO 9001:2000
Focus?	Alle activiteiten en beheersmaatregelen van de service-organisatie die de bedrijfsvoering van de gebruikersorganisatie beïnvloeden (risico management).	Alle activiteiten en beheersmaatregelen die de door de klant ervaren kwaliteit bepalen. (kwaliteitsmanagement)
Eigenaar?	American Institute of Certified Public Accountants (AICPA)	International Organisation of Standardization (ISO)
Certificatie?	Een SAS 70 audit levert geen certificaat op. Opgeleverd wordt een rapport met daarin opgenomen de verklaring van de auditor ten aanzien van de opzet en operationele effectiviteit van de beheersmaatregelen.	De audit resulteert in een certificaat.
Uitvoering?	De audit voor SAS 70 wordt uitgevoerd door een Register Accountant.	De audit voor ISO 9001 wordt uitgevoerd door een gekwalificeerde auditor, via een geaccrediteerde certificatie-instelling.
Doel van het rapport?	(Potentiële) opdrachtgevers een onafhankelijk oordeel bieden dat de dienstverlening 'in control' plaats vindt	Vaststellen dat de organisatie in staat is aan eisen en wensen van klanten en van toepassing zijnde wet- en regelgeving te voldoen.
Aard van het rapport?	Rapport geeft zekerheid omtrent het bestaan en het passende ontwerp van de door de service-organisatie gepresenteerde beheersmaatregelen. In het geval van een Type 2-verklaring wordt er ook uitsluitsel gegeven over de effectiviteit ervan.	Certificaat geeft aan dat de organisatie in staat is met klantenwensen en van toepassing zijnde wetgeving om te gaan.
Houdbaarheid van het rapport?	Type 1 is een momentopname, Type 2 bestrijkt ten minste een periode van zes maanden waarin uitgebreid gemeten en getoetst is en is een jaar geldig.	Het certificaat moet om het jaar getoetst worden en is drie jaar geldig.
Normering van beheersdoelstellingen en activiteiten?	Nee, wel een verplichte hoofdstukindeling voor het rapport.	Ja, vijf hoofdstukken met eisen ten aanzien van de inrichting van het kwaliteitsmanagementsysteem.
Onderwerpen?	SAS 70 kent geen vaste normen en standaarden. Het SAS 70 rapport is maatwerk en service-organisatie en gebruikersorganisatie zijn (in onderling overleg) vrij om te bepalen welke beheersdoelstellingen en processen worden meegenomen in het onderzoek. Als handvat worden vaak wel de COSO componenten Control Environment, Risk Assessment, Information and Communication and Monitoring gebruikt!	Vijf hoofdstukken: 1. Eisen aan het kwaliteitsmanagementsysteem; 2. Verantwoordelijkheid van het management; 3. Management van middelen; 4. Klantgerelateerde processen; 5. Meting, analyse en verbetering.
Aanvullende bevindingen en aanbevelingen?	Ja, opgenomen in de rapportage Type 2.	Niet standaard. Sommige certificeerders voegen bevindingen en aanbevelingen bij, naast de reguliere documentatie.
Rapport gericht op ...?	Het management en de externe accountant van de gebruikersorganisatie.	Management en klanten van de organisatie.
Nut rapport in relatie tot jaarrekening?	Wanneer het uitbestede proces is gekoppeld aan materiële posten van de jaarrekening, verschaft het SAS 70 rapport de accountant van de gebruikersorganisatie inzicht in de kwaliteit van de procesbeheersing bij de service-organisatie.	Geen. Het ISO 9001-certificaat wordt niet erkend als een geldig 'third party audit report'.
Target clients?	Ieder bedrijf dat een dienst verleent voor een opdrachtgever met impact op de beheersdoelstellingen en/of de jaarrekening.	ISO 9001 is een generiek model, toepasbaar op iedere organisatie.
Target industries?	Financiële dienstverlening, Verzekeringen, Gezondheidszorg en IT.	Geen beperking.

Afbeelding 4: ISO 9001 en SAS 70 – verschillen en overeenkomsten.

Biedt SAS 70 de voordelen van het ISO 9001-certificaat?	
Voordelen ISO 9001-certificaat	SAS 70?
ISO 9001 is een generiek model, toepasbaar op vrijwel iedere soort organisatie onafhankelijk van omvang of product/dienst (van kippenslachterij tot makelaarskantoor).	Het SAS 70 rapport is altijd maatwerk, afgestemd met een individuele opdrachtgever of een groep (potentiële) opdrachtgevers.
ISO 9001 is een begrip in de (internationale) markt. Hoge mate van naamsbekendheid en erkenning van toepassing ervan.	SAS 70 is een begrip in de wereld van grote, veelal internationale serviceverleners. Ook bedrijven die te maken hebben met Sarbanes-Oxley zijn ermee bekend.
Het ISO 9001-certificaat geeft soms toegang tot markten die zonder certificaat niet bediend zouden mogen worden.	Inmiddels is een SAS 70 rapportage binnen de financiële wereld een must. Vooral wanneer er sprake is van relaties met de Amerikaanse markt.
ISO 9001 biedt met het onderliggende procesmodel goede aanknopingpunten voor organisatieverbetering en verbetering van de klantgerichtheid.	SAS 70 heeft geen onderliggend procesmodel, maar vanwege de verplichting om op procesniveau beheersdoelstellingen te formuleren en die te toetsen (wat wil de klant, en slagen we daarin?) worden verbeterkansen goed zichtbaar.
Biedt SAS 70 een oplossing voor de nadelen van het ISO 9001-certificaat?	
Nadelen ISO 9001-certificaat	SAS 70?
ISO 9001-certificatie krijgt niet altijd de aandacht van het management die ze verdient. ISO is bij sommige organisaties vooral iets van de kwaliteitsmanager. Hierdoor wordt verbeterpotentieel onbenut gelaten.	SOX is 'hot', en SAS 70 dus ook: beide methodieken hebben in de financiële wereld een dusdanige status dat het management ze niet kan negeren. Dit betekent dat verbeterinitiatieven van SOX en SAS zich makkelijker op de management-agenda laten plaatsen.
Vaste set van voorschriften en criteria die als geheel dienen te worden geïmplementeerd. Afwijken van deze basisset betekent dat er niet kan worden gecertificeerd. Dit kan resulteren in een 'papieren tijger': veel papier met weinig effect.	Maatwerk: Op basis van overleg met de opdrachtgever worden de beheersdoelstellingen per proces bepaald die vervolgens worden getoetst. Opdrachtgever heeft dus grote invloed op het beheersinstrumentarium van de service-organisatie. De maatregelen zijn ook belangrijker dan de procedures. Procedurebeschrijvingen zijn niet noodzakelijk, zodat er met minder papier kan worden volstaan.
Er is variatie in kwaliteit en deskundigheid bij certificatie-bureaus en auditors met effect op zeggingskracht van het certificaat en toegevoegde waarde van de audit voor de organisatie.	Toezicht op en kwaliteitsbeheersing van Register Accountants is zeer strikt, niet in de laatste plaats vanwege de schandalen van de afgelopen jaren. Dit heeft een positief effect op de waarde van het SAS 70 rapport.

Afbeelding 5: Voordelen en nadelen.

samenwerking, toezicht of begeleiding van de externe accountant. Naar opvatting van de auteur is de zekerheid die aan een SAS 70 rapport kan worden ontleend dan ook groter dan ontleend aan een ISO-certificaat.
Een SAS 70 rapport kan op maat gemaakt worden voor een groep (potentiële) opdrachtgevers. De praktijk leert dat op deze wijze een SAS 70 rapport inzet kan worden van contractonderhandelingen en dus ook een commerciële rol kan spelen.

Conclusie

Het ISO 9001-certificaat en het SAS 70 rapport spelen op dit moment een belangrijke rol in verschillende bedrijfstakken en zijn dus zeker niet zomaar uitwisselbaar. Er is wel een aantal alternatieve scenario's denkbaar. Het eerste: de methodiek van SAS 70 zou kunnen worden gebruikt binnen een ISO 9001-certificaat voor wat betreft hoofdstuk 7.4: Inkoop. De gecertificeerde organisatie gebruikt in dat geval de vraagstelling van SAS 70 om haar leveranciers inzicht te laten verschaffen in hun bedrijfsproces.
Het tweede: de methodiek van SAS 70 zou kunnen worden gebruikt als aanvulling op ISO-certificatie door de eis 'Bewaking en meting van processen (8.2.3)' met de vraagstelling vanuit SAS 70 in te vullen. Per proces zouden op basis van workshops met vertegenwoordigers van de belangrijkste klanten beheersdoelstellingen kunnen worden opgesteld, vergezeld van een meetmethodiek om die doelstellingen te monitoren.
Het derde: in een markt of bedrijfstak waar (nog) geen sprake is van een dominante kwaliteitsstandaard kan een organisatie zowel kiezen voor SAS als voor ISO. Belangrijkste afwegingen zijn dan maatwerk of generiek, Register Accountant of Quality Auditor, kwaliteitssysteem of risico management, en momentopname of uitgebreide tests.

Samenvattend kan worden gesteld dat de keuze voor SAS of ISO in hoge mate zal worden bepaald door marktomstandigheden. Een organisatie zal die kwaliteitsstandaard kiezen die binnen de eigen bedrijfstak het best geaccepteerd is of de meeste status heeft.
De auteur heeft de voorkeur voor het SAS 70 rapport. De methodiek is zeer klantgericht, de rapportage is zeer goed onderbouwd, de kwaliteit van de externe accountant staat nauwelijks ter discussie en 'meten is weten' biedt de beste mogelijkheden voor proces- en organisatieverbetering.

Robert Klingens
Drs. R.V.A. Klingens is proces manager bij een grote pensioenverzekeraar.
Met dank aan Drs. R. van Berkel RA.