

UITBESTEDEN VAN DE F&A FUNCTIE

In de ogen van menig bedrijf dat zijn financiële en administratieve (F&A) processen wil uitbesteden, biedt een SAS 70-verklaring alleen onvoldoende houvast om actief de verwachte opbrengsten en risico's te beheersen. Een kijkje in de compliance-keuken van financiële dienstverleners kan uitkomst bieden. Beheersing of 'control' is namelijk iets wat financiële instellingen als geen ander onder de knie hebben.

Betere performance en control

In *Het Financieele Dagblad* van maandag 22 oktober 2007 staat dat toenemende regelgeving en complexiteit voor pensioenfondsen belangrijke drijfveren zijn om verschillende bedrijfsactiviteiten uit te besteden. Volgens het artikel hebben Nederlandse pensioenfondsen voor 100 miljard euro aan pensioenvermogen ondergebracht bij derden. De bedragen behorend bij het uitbesteden van financiële en administratieve (F&A) processen zijn weliswaar minder indrukwekkend, maar de trend is dezelfde: steeds meer organisaties besluiten (delen van) de F&A-functie uit te besteden.

De uitdagingen waar een pensioenfonds bij outsourcing voor staat, zijn voor een deel gelijk aan de thema's en risico's voor een willekeurig andere organisatie die F&A-processen wil uitbesteden. Dit artikel biedt handreikingen aan degene die wil uitbesteden en vindt dat een SAS

70-verklaring alleen onvoldoende houvast biedt om actief de verwachte opbrengsten en risico's te beheersen. Hiertoe combineert dit stuk een kijkje in de compliance-keuken van financiële dienstverleners met een dosis pragmatisme. Beheersing of 'control' is namelijk iets wat financiële instellingen als geen ander onder de knie hebben vanwege het woud van wet- en regelgeving waarover aan toezichthouders zekerheid dient te worden afgegeven.

Verlies van controle is een belangrijk punt van zorg bij menig bedrijf dat het outsourcingpad op gaat. Veel organisaties maken gebruik van een Statement of Auditing Standards nummer 70 (SAS 70)-verklaring om greep te houden op de interne beheersingsmechanismen en -processen van leveranciers. Een SAS 70-verklaring is echter geen wondermiddel en al helemaal niet goedkoop.

Om bruikbaar te zijn dient de scope van de verklaring te worden vastgesteld in nauw overleg met de uitbestedende organisatie. Wordt dit overgelaten aan de leverancier, dan is

de kans groot dat deze de beheersingsmaatregelen ('controls') zal kiezen waar hij zich prettig bij voelt. De eerste aanbeveling is dan ook dat zowel de interne afnemers van de F&A-dienstverlening als de eigen afdeling worden betrokken bij het definiëren van de dienstverlening en beheersmaatregelen die gecontracteerd worden met de leverancier.

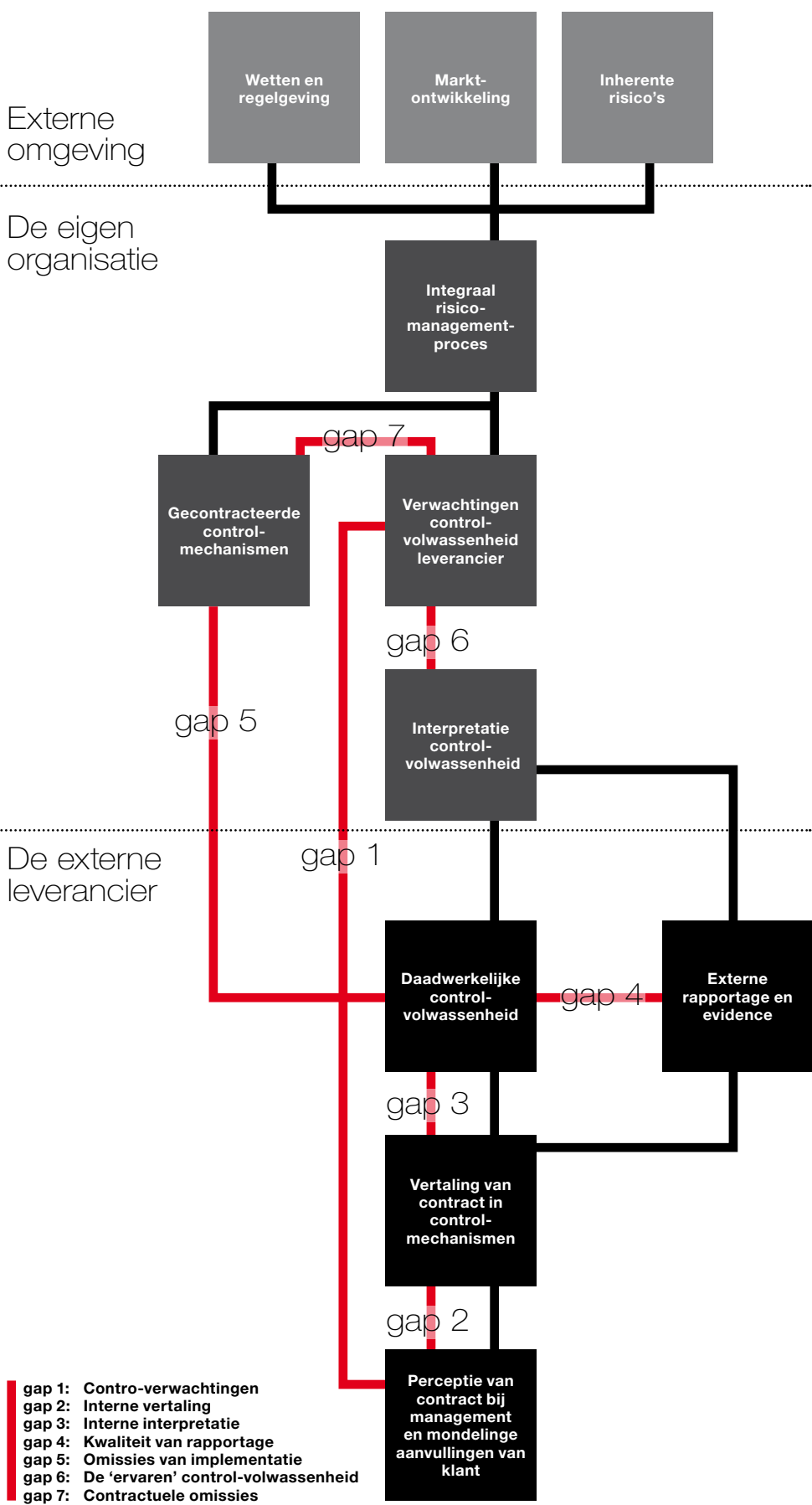
Een fundamentele tekortkoming van een SAS 70-verklaring is dat deze onvoldoende waarborgen biedt om een situatie te voorkomen waarin de geleverde dienst onvoldoende aansluit bij de behoeften en verwachtingen van de uitbestedende organisatie. Een SAS 70-verklaring richt zich namelijk op het toetsen of de leverancier bepaalde activiteiten gecontroleerd uitvoert en minder op het eindresultaat. Een effectieve en efficiënte aansturing van de leverancier, zowel vanuit bedrijfsvoerings- als vanuit regelgevingsperspectief, vraagt dan ook om meer dan alleen een jaarlijkse (dure) verklaring van een accountancybureau.

WAAR KAN HET FOUT GAAN

Twee eisen betreffende outsourcing die in bijna alle wet- en regelgeving gericht op financiële dienstverleners terugkomen zijn: 1) de partij die de dienst uitbesteedt, blijft eindverantwoordelijk, en 2) de uitbestedende partij dient bij de toezichthouder te kunnen aantonen dat zij voldoende zekerheid kan bieden over de interne beheersing van haar leveranciers.

Voor de niet-financiële instelling die de F&A-processen wil uitbesteden, bieden beide eisen een goed startpunt voor het definiëren van de interne regiefunctie en de risicomanagementelementen in het contract. Welke risico's gemitigeerd dienen te worden varieert per fase van de uitbesteding. Omdat tijdens de selectie- en contracteringsfase het fundament wordt gelegd voor de rest van de levenscyclus, is het cruciaal om in deze fase voldoende ver vooruit te kijken. In de praktijk ligt de nadruk tijdens de contractering echter vooral op het contractueel wegmanagen van zo veel mogelijk (financiële) risico's. Het eindresultaat is een statisch en op het eerste gezicht goedkoop contract. Het mitigeren van risico's is echter een complex en dynamisch onderwerp en is dus gebaat bij flexibiliteit. Onderschatting hiervan kan dan ook leiden tot 'goedkoop is duurkoop'.

Wat de materie complex maakt, is weergegeven in de figuur op de volgende pagina. Hierin worden omgevingsfactoren op schematische wijze vertaald in een control-raamwerk om de



uitbesteding te beheersen. De vertaling vindt allereerst plaats via een interpretatie van de eisen door de uitbestedende organisatie, gevolgd door een interpretatie van de voorgenoemde interpretatie door de externe leverancier. In dit licht bezien is het niet vreemd dat de controlvolwassenheid niet in alle gevallen aansluit bij de verwachtingen.

De tweede aanbeveling is dan ook om de (financiële) invloed van wet- en regelgeving al tijdens het opstellen van de initiële businesscase mee te nemen. Invloed op zowel het ontwerp van de eigen regiefunctie als de eisen waar de leverancier aan dient te voldoen, moet worden meegenomen in de kwalitatieve en kwantitatieve analyses. Dit, in combinatie met voldoende ruimte in het contract om in te spelen op bijvoorbeeld wijzigingen in wet- en regelgeving en 'hidden services', moet voorkomen dat beide partijen binnen een à twee jaar na ondertekening met een gespannen relatie zitten. Met andere woorden:

EEN GOEDE VOORBEREIDING...

Voorkomen dat risico's tot verrassingen leiden vereist onder andere dat de leverancier de eisen moet kunnen meenemen in het (financiële) aanbod dat hij uitbrengt naar aanleiding van het Request for Proposal of Request for Quotation. Hiertoe dient 'risicomanagement' als een volwaardige dienst omschreven te worden, inclusief key control indicators, control service levels en eisen aan rapportages. Een belangrijk aandachtspunt bij het omschrijven van de dienst vanuit zowel effectiviteit als efficiency is het classificeren van de benodigde controls als black of white box.

Het managen vanuit black box-perspectief betekent dat de uitbestedende organisatie een deel van de benodigde control objectives zodanig definieert dat de leverancier erover rapporteert, maar het voor de uitbestedende organisatie niet noodzakelijk is om te weten hoe de leverancier de beheersmaatregelen intern organiseert. Andere risico's vereisen wel kennis van de interne werking om te waarborgen dat het risico aansluit bij de risicotolerantie van de uitbestedende organisatie. Deze risico's worden geclassificeerd als black box.

sificeerd als white of glass box. Twee eenvoudige voorbeelden om het iets tastbaarder te maken.

1 Een van de technologiegerelateerde risico's is de kwaliteit van de financiële data opgeslagen in de IT-systemen van de leverancier. De uitbestedende organisatie moet eisen stellen aan de data in termen van integriteit, beschikbaarheid en vertrouwelijkheid, omdat anders niet vertrouwd kan worden op de financiële gegevens. Hoe de leverancier dit vervolgens inregelt is minder relevant, zolang de leverancier kan aantonen dat er adequate controls zijn ingericht.

Manage dit risico dan ook als een black box.

2 Vanuit de uitbestedende organisatie is een specifiek leveranciersrisico het niet beschikbaar zijn van uitbestede

personeelsleden die beschikken over waardevolle bedrijfsinformatie ('key personnel'). Om dit risico te mitigeren zal de uitbestedende organisatie het interne besluitvormingsproces van de leverancier om zo iemand te vervangen actief willen beïnvloeden. Dus classificeren als een white box.

De controls- en rapportagestructuur gedefinieerd als onderdeel van het contract met de leverancier dienen geborgd te worden binnen de regiefuncties van zowel de leverancier als de uitbestedende organisatie. Daarnaast dient de uitbestedende organisatie de contractueel vastgelegde controls te verankeren binnen het bedrijfsbrede risicomanagementproces om te waarborgen dat de F&A-risico's afdoende beheerst worden. Deze aanpak heeft als voordelen dat de uitbestedende organisatie over recentere en goedkopere informatie beschikt in vergelijking met een jaarlijkse SAS 70-verklaring. Voor die onderdelen waar het resterende risico nog als te hoog wordt geschat, kunnen additionele mitigerende maatregelen getroffen worden, waaronder een SAS 70-verklaring. Deze verklaring heeft dan echter een veel beperktere scope en dus dito lagere kosten.

VAN RISICOBEPERKING NAAR WAARDECREATIE

Het opnemen van een risicomanagementdienst als onderdeel van het contract en het implementeren van outsourcing-risicomanagement (ORM) binnen de eigen regieorganisatie is de derde aanbeveling, waarbij voor het implementeren van ORM geleund kan worden op het bestaande risicomanagementkader. Deze basisset aan controls kan vervolgens aangevuld worden met controls afgeleid van specifieke eisen die in relevante wet- en regelgeving aan uitbesteding van F&A-

Control-volwassenheid sluit niet in alle gevallen aan bij de verwachtingen

processen worden gesteld.

Voor welke risico's welke mitigerende maatregelen getroffen dienen te worden, hangt af van de gevolgen van een onwenselijke gebeurtenis en de kans dat deze optreedt. Een voorbeeld: de financiële gevolgen van het niet op tijd kunnen factureren aan klanten door een verstoring in een financieel IT-systeem beheerd door een leverancier, kunnen bepaald worden door de opportunity- en rentekosten te berekenen. Door dit vervolgens af te zetten tegen het maximale schadebedrag dat de uitbestedende organisatie acceptabel vindt, kan een besluit genomen worden over het accepteren, mitigeren of overdragen van het risico.

In de praktijk ligt de nadruk van risicomanagement bij outsourcing helaas nog te vaak op het puur signaleren van tekortkomingen bij de leverancier. Zou het niet mooi zijn als enerzijds de beheersingsmechanismen van de externe leverancier en anderzijds het definiëren van controls die de leverancier stimuleren om een meetbaar hogere kwaliteit te leveren, onderdeel gaan uitmaken van een integrale benadering van risicomanagement? Voor een voorbeeld met betrekking tot een control waardoor de leverancier gedwongen wordt een risico te beheersen en tegelijkertijd de kwaliteit te verhogen,

wordt teruggegrepen op het eerder genoemde technologierisico dat de kwaliteit van de door de leverancier beheerde financiële data niet adequaat is. Om IT-risico's te mitigeren wordt vaak gerefereerd aan zogenaamde 'general IT controls'. De twee meest relevante general IT controls die het risico van niet-beschikbaar zijn van data moeten verminderen, schrijven voor dat 1) de IT-leverancier een probleemmanagementproces moet inrichten om te reageren op ongewenste situaties, en dat 2) er service levels afgesproken en gemonitord worden. Dit is een typische white box-oplossing, met het bijbehorende nadeel dat er gefocust wordt op het hoe en minder op het eindresultaat.

Een betere control is er een die zich richt op het verminderen van het aantal verstoringen en/of de gemiddelde duur van een verstoring met een voorgedefinieerd jaarlijks percentage. Een van de controls voor de leverancier wordt dan: 5 procent minder incidenten in de komende twaalf maanden. Op het al dan niet behalen van dit resultaat stuurt vervolgens de regiefunctie van de uitbestedende organisatie.

Om de voornoemde control te realiseren moet de leverancier onder andere een proces inrichten, intern rapporten, iemand verantwoordelijk maken et cetera. Dit alles is voor de uitbestedende organisatie echter geen relevante informatie. Het gaat de uitbestedende organisatie ten slotte om de performance in voor haar relevante meetbare eenheden. Een bijkomend voordeel van deze aanpak voor de uitbestedende organisatie is dat minder verstoringen leiden tot meer tijd om omzet te maken met dezelfde middelen, of dezelfde omzet met minder middelen. ■

✉ **FRANÇOIS ZIELEMANS** (francois.zielemans@protiviti.nl) is manager bij Protiviti en gespecialiseerd in uitbestedingsvraagstukken en het inrichten van regieorganisaties. Dit artikel is gebaseerd op een white paper die het mitigeren van eisen vanuit regel- en wetgeving binnen de bancaire en verzekeringswereld in meer detail beschrijft. Deze white paper is beschikbaar gesteld op www.protiviti.nl.