SPRENKELS & VERSCHUREN
ACTUARISSEN CONSULTANTS

RiskTransparant, deel 2

De waarde van een ISAE rapport?

"…welke waarde heeft een ISAE voor het bestuur: in control of een illusie van control…"

In deze tweede serie uit een reeks van zeven delen, delen wij graag onze kennis met u over risicomanagement. Dit keer staat het dossier: "de waarde van een ISAE" centraal.

Vijf jaar van ISAE, juni 2011 - juni 2016

Juni 2011, was de datum dat de SAS 70 *(Statement on Auditing Standards, nr. 70, service organisations)*, werd vervangen door de ISAE *(International Standard on Assurance Engagements nr. 3402)*, door de IAASB *(International Auditing and Assurance Standards Board)*. Nu exact vijf jaar later is de vraag of het een proces is geweest van: 'in control' of een 'illusion of control'?

Inleiding

In o.a. het jaarwerkproces wordt gesteund op de ISAE door de externe accountant voor de mate van interne beheersing. De vraag is of elk fonds er 'zomaar' vanuit kan gaan dat er sprake is van 'in control' of is er sprake van een 'illusie van control'? Na de zomermaanden is de agenda weer gericht op 2017. Staat de ISAE daar ook op of is het een automatisch gegeven en een rapport dat niet echt wordt doorgenomen?

In deze tweede editie van RiskTransparant, geven wij u onze visie en een aanpak voor een waarde creërend ISAE proces, dat intrinsiek bijdraagt aan een beheerste en integere bedrijfsvoering.

Als bestuur bent u verantwoordelijk voor uw bestuursprocessen en ook de (primaire en secundaire) uitbestede processen in het perspectief van een beheerste en integere bedrijfsvoering. Steeds vaker zien wij dat er meer uitbesteed wordt aan specialisten op één bepaald terrein (een niche). Dit was al het geval voor vermogensbeheer en nu bijvoorbeeld ook voor de communicatie met deelnemers via de website. Ook het fenomeen 'onderuitbesteding' komt vaker voor. In dit geval worden (deel)processen uitbesteed aan andere partijen onder de verantwoordelijkheid van een hoofduitvoerder. Het samenspel in de keten wordt hierdoor complexer en het is van groot belang om de balans in de keten, in termen van risico en rendement, goed te blijven volgen. Deze taak ligt á priori aan de bestuurstafel, ook vanuit een (compliance) wettelijk perspectief. Zo geven o.a. de artikelen 34 en 143 van de Pensioenwet duidelijke ankerpunten mee voor uitbesteding en integere bedrijfsvoering. Hiermee heeft de wetgever voorzien in een proces van verantwoordelijkheid voor bestuurders. De volgende vragen kunnen nu worden gesteld: wanneer is er sprake van een beheerste en integere bedrijfsvoering? Welke maatstaf hanteert u aan de bestuurstafel? Welke maatstaf hanteren toezichthouders en andere stakeholders? Om deze vragen te beantwoorden is een zogenoemde intern en extern normenkader nodig. Voor een beheerste en integere bedrijfsvoering verwacht DNB ook dat u onafhankelijk een mening kunt vormen over de interne controle en beheersingssystemen van uw uitvoerder en onderuitvoerders. U moet zicht en inzicht hebben op de hele keten.

De focus van dit artikel ligt op de ISAE. De ISAE op zichzelf kent geen vooraf gedefinieerd normenkader. Dit is wel wat vaak wordt verondersteld. Het hebben van een normenkader is van groot belang. Immers een auditor heeft een (intern of extern (wettelijk)) normenkader nodig om zijn werk te doen én aan de bestuurstafel moet overeenstemming zijn over het gewenste

volwassenheidsniveau van de (uitbestede)processen. De vraag die hieruit voortvloeit is of u als bestuurder een normenkader heeft vastgesteld? Het tastbaar maken van een bruikbaar normenkader kan een lastige opgave zijn.

Als leidraad kunt u de volgende onderdelen meenemen:
1. Relevantie
2. Betrouwbaarheid
3. Begrijpelijkheid
4. Volledigheid
5. Neutraliteit

Het is verder van belang om te begrijpen welke methode van ISAE het bestuur wenst te hebben:
1. Inclusive methode
2. Carve out methode

De '*inclusive* methode' schrijft voor dat indien de service organisatie processen zelf weer heeft uitbesteed ook deze processen integraal opgenomen moeten worden. Dit noemen we de sub-serviceorganisatie, de onderuitvoerder. Indien uw uitvoeringsorganisatie bijvoorbeeld het proces van ex-casso heeft uitbesteed, dan dienen de beheersmaatregelen van deze partij opgenomen te zijn.

Bij de '*carve out* methode' worden de beheersmaatregelen van de sub-service organisatie niet opgenomen in het ISAE rapport. Er wordt vaak verwezen naar het rapport van de sub-service organisatie.

In de pensioensector zien wij vaak de toepassing van de zogenoemde 'carve out methode'. Dit betekent dat het bestuur alert moet zijn op de assurance in de keten van alle partijen. Het hebben van een ISAE voor alleen een service organisatie, indien er sprake is van een sub-service organisatie, is hiermee niet voldoende. Het bestuur moet er ook alert op zijn dat er vaak sprake is van een generiek ISAE en geen fondsspecifiek rapport. Weet u of in de steekproef ook uw deelnemersadministratie is meegenomen bij een generiek rapport? En zijn er voor uw fonds specifieke zaken die niet in scope van de ISAE zijn? Kortom, is het rapport representatief voor uw situatie en begrijpt u de beperkingen in de reikwijdte?

Naast de methodes, als hierboven omschreven is het van belang om te begrijpen welke type ISAE rapportages er zijn. Er zijn twee types: I en II.
1. Type I: gaat over de opzet en bestaan.
2. Type II: gaat ook over de werking.

Type I: betreft een momentopname. Hierin wordt beschreven hoe het proces en de beheersingsmaatregelen zoals deze op een bepaald moment zijn geïmplementeerd. Door de auditor wordt de toereikendheid getoetst van de beschreven beheersingsmaatregelen in relatie tot de doelstellingen. Dit type rapport moet worden gezien als informatief rapport. Doordat de werking niet is opgenomen kan er geen oordeelsvorming plaatsvinden over de uitkomsten van het proces.

Type II: betreft een periode, meestal zes maanden tot een jaar. Dit type rapport beschrijft de opzet, bestaan én werking van de beheersingsmaatregelen gedurende de gedefinieerde periode en of deze effectief zijn geweest. Dit type rapport zou het uitgangspunt moeten zijn voor elk fonds naar hun uitvoeringsorganisaties. Juist ook omdat een pensioenfonds zijn eigen 'volwassenheid' van beheerste en integere bedrijfsvoering moet aantonen aan haar

stakeholders. Zo verlangt DNB dat er sprake is van een volwassenheid van drie op de maturiteitsladder van vijf. Door alleen een Type I rapport, kan hier al niet aan worden voldaan.

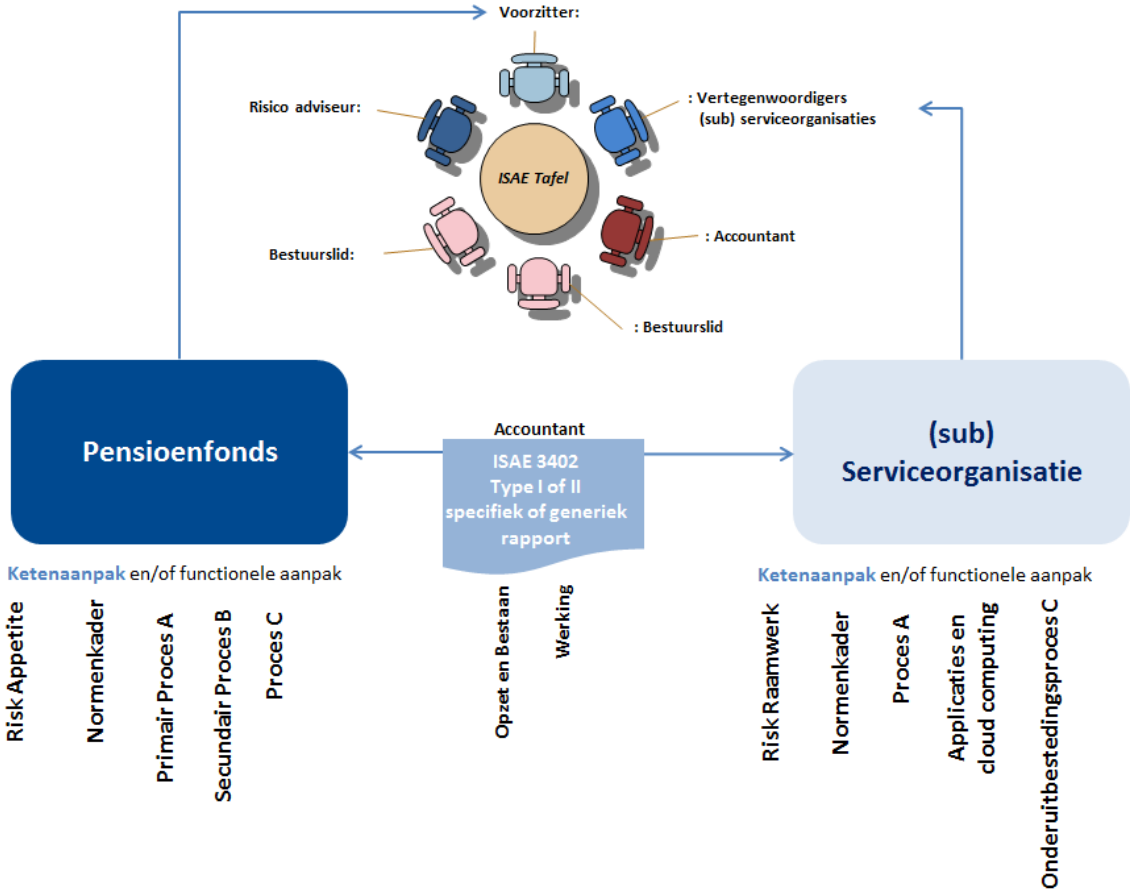
Er zijn twee vragen die vaak gesteld worden: *wat te doen én hoe te doen?* Deze twee vragen staan centraal in deze RiskTransparant.

Wat te doen?

Door regelmatig stil te staan bij de volgende 5 vragen, kunt u inzicht en bewustwording verkrijgen c.q. vergroten:

1. Hebben wij als bestuur ex-ante een normenkader opgesteld passend bij onze risicobereidheid, waaraan ons ISAE moet voldoen en welk type rapport wensen wij, generiek of fondsspecifiek?
2. Welke methode willen wij: inclusive of carve out?
3. Welke (IT)processen dienen in scope te zijn van onze ISAE? Is dit nu ook al het geval?
4. Zijn er of zien wij aankomende veranderingen in onze doelstellingen die een impact hebben op onze processen? Zo ja, welke processen zijn dit, welke systemen worden hierdoor geraakt en zijn deze opgenomen in de scope van onze ISAE?
5. Hebben wij de juiste riskgovernance inrichting, waarbij het proces van opzet, bestaan en werking, inclusief monitoring en evaluatie voor de hele uitbestedingsketen is belegd?

Figuur 1: ISAE risk governance, als onderdeel van uw risicomanagement commissie



Nu de *wat* vraag is besproken, maken wij een doorkijk naar de *hoe* vraag.

Hoe te doen?

De eerste stap is om uw uitgangspunten en hiermee een normenkader te bepalen voor uitbesteding. Dit gaat dan ook om uw eigen inzichten, rekening houdend met de wettelijke kaders.
Om dit proces gestructureerd te laten verlopen kunt u o.a. het *best practice* RAVC© model hanteren. Dit geeft u houvast in het proces, geeft duidelijk structuur en verhoogt het risicobewustzijn op dit onderdeel. Dit is van groot belang om ook een zogenoemd 'internal control statement' van de uitvoerder goed te kunnen interpreteren. Indien er vooraf geen sprake is van een normenkader én geen ex-ante risicobereidheid (risk appetite) is, is de samenhang met een ex-post internal control statement lastig te leggen.

De tweede stap is om (minimaal) binnen uw risicomanagement commissie een proces en inrichting te hebben van risk governance voor (ook) de ISAE. Hiernaast is het creëren van samenhang met de andere tafels binnen het bestuur van belang, zoals beleggingscommissie, communicatiecommissie en actuariële commissie. Immers de processen van deze commissies maken (vaak) onderdeel uit van de uitbestede activiteiten. Naast de interne governance is het ook van belang om begrip te hebben hoe de risk governance van de uitvoerder is ingeregeld naar de deelnemersketen en werkgeversketen. Hoe versterkt deze governance uw governance? Vragen die van belang zijn, zijn o.a.:

- Welk proces van risk management wordt doorlopen bij de uitvoerder?
- Wat is de samenhang van de compliance officer met de risicomanagement functie?
- Is er een internal audit afdeling en is deze onafhankelijk of is er sprake van rapportage aan een interne riskmanager?

De derde stap is het bepalen van de scope van de ISAE in relatie tot uw normenkader. Hiermee kan de ISAE elk jaar van scope wijzigingen of kan er een incidenteel een extra audit gedaan worden. Uw begrip van de veranderingen in processen (materialiteit en/of cumulatie) is van wezenlijk belang voor de uit te voeren ISAE-audit. Wanneer heeft u voor het laatst de scope besproken met uw uitvoerder?

De vierde stap is om na te gaan welke deficiënties er geconstateerd zijn. Hoe worden deze opgevolgd door de uitvoerder? Zijn er ook terugkomende zaken als bijvoorbeeld: juistheid, tijdigheid en accuraatheid van verwerkingen of tijdig signaleren van bijzondere gebeurtenissen of zijn er deficiënties ten aanzien van IT in:

- Informatiebeveiligingsbeleid
- Toegang tot systemen (fysieke toegangsbeveiliging)
- Toegang tot applicaties en gegevens (logische toegangsbeveiliging)
- Wijzigingsbeheer
- Incident management
- Beschikbaarheid
- Continuïteit en operationeel beheer

Maar ook het proces van het opstellen en correct archiveren van mutatiebrieven, dient in orde te zijn. Welk proces vindt u materieel en welk proces vindt u minder materieel?

De vijfde stap is om een zogenoemde ISAE Score Card in te richten in een verantwoordingscyclus. Dit helpt u om een verantwoord proces in te richten.

Figuur 2: ISAE Risk Based Score Card

Processtap	Doel van deze stap	Korte toelichting
Vertrekpunt 1	**Bepalen Ex-Ante uitgangspunten van het Bestuur voor ISAE**	• *Startpunt is uw visie en ambitie en op basis hiervan de door u afgesloten Service Level agreement, als vertrekpunt.* • *Hoe controleert u de serviceorganisaties op compliance?* • *Wenst u een generiek of fonds specifiek ISAE?* • *Hoe controleert u de interne organisatie (gebruikersorganisatie) op eigen verantwoordelijkheden in relatie tot uitbesteding (user control consideraties)?* • *Heeft u uw Risk Appetite hiervoor vooraf vastgelegd, met bv de RAVC © methode?* • ***Kortom: Wat is uw normenkader en welke methode van ISAE wenst u?***
Versterken 2	**Bepalen effectieve Risk Governance**	• *Heeft de serviceorganisatie een adequate inrichting van Risk Governance?* • *Welke organisatie inrichting heeft de serviceorganisatie en is deze representatief voor uw organisatie?* • *Wat is de samenhang in de totale keten*

		van serviceorganisaties ten opzichte van de gebruikersorganisatie? Wie kijkt naar de totale keten over alle serviceorganisaties heen?
Verdiepen **3**	**Bepalen Risk & Control assessment**	• *Is er op basis van de juiste scope een risk assessment uitgevoerd?* • *Welke steekproef is gehouden door de accountant?* • *Zijn de controls goed gedefinieerd en getest?* • *Zijn de veranderingen in de organisatie meegenomen, die een impact kunnen hebben op de scope en dienstverlening?*
Verankeren **4**	**Ex Post Monitoren en Evalueren**	• *Welke deficiënties zijn er geconstateerd door de externe accountant?* • *Hoe worden deze opgevolgd door de serviceorganisatie?* • *Welke rapporten zijn er van de interne auditoren over de dienstverlening en IT?* • *Komen de reikwijdte, periode en beheersdoelstellingen overeen met de rapportage periode en gewenste reikwijdte en beheersing?* • *Zijn de eventuele onderuitbestedingen meegenomen?*
Verantwoorden **5**	**Bepalen hoe te rapporteren en of de hele keten qua assurance inzichtelijk is gemaakt, door middel van een ISAE Risk Based Score Card**	*Kan er gerapporteerd worden naar de volgende vier onderdelen:* • *Scope en volledigheid* • *Assurance in de keten* • *Effectiviteit van Risk Governance* • *Effectiviteit van Risk Management*

Kortom: in 5 concrete stappen naar een hoger vertrouwen in uw fonds!

Meer informatie óf meer kennis delen?

Download de andere artikelen op www.sprenkelsenverschuren.nl of neem contact op met uw vaste contactpersoon bij Sprenkels & Verschuren, zo ook voor:

RiskTransparant, deel 1: Het IT dossier is een must voor elke Bestuurder – uitgave mei 2016

Over Sprenkels & Verschuren

Sprenkels & Verschuren heeft circa 50 professionals, strategische adviseurs en ontwerpers van financiële en niet financiële modellen. Sprenkels & Verschuren geeft niet alleen advies maar implementeert ook. Wij zijn denkers en doeners. Wij delen én ontwikkelen kennis graag in co-creatie. Waarom? Omdat elk antwoord een vraag is geweest én geen enkele vraag hetzelfde is.