Houd regie bij uitbesteding

Het beheersen van de uitvoering van een pensioenfonds, waaronder de uitbesteding en IT, blijft een uitdaging. Als bestuur ben en blijf je verantwoordelijk voor de totale keten, maar welke informatie heb je nu nodig om in control te komen en te blijven in een snel veranderende (pensioen)wereld? De snelheid waarmee nieuwe en vernieuwde inzichten ontstaan is hoog. Uitbesteding en IT in brede zin zijn ook onderwerp van nieuwe wet- en regelgeving. Hoe zorgen we er dan voor dat deze ontwikkelingen worden geïntegreerd in bestaand beleid en uitvoering, zonder dat wildgroei of onvoldoende geïntegreerd beleid ontstaat? Het is goed om als bestuur terug te gaan naar de basis en van daaruit de organisatie van het pensioenfonds te verstevigen.

De basis van een pensioenfonds ligt vast in de missie, visie en strategie, die vervolgens nader zijn uitgewerkt in doelstellingen. Telkens als zich nieuwe inzichten en ontwikkelingen voordoen moeten deze worden ingebed, passend bij de doelstellingen van het fonds. Bij deze inbedding moeten vragen worden beantwoord als: Waarom is er sprake van een nieuw inzicht? Wat willen we voorkomen en wat voor aanpassingen zijn daarvoor nodig? Hoe passen deze in bestaand beleid en de totale bestuurscyclus? Vragen die moeten worden gesteld en beantwoord om de integrale beleidsstructuur te behouden.
In dit artikel beschrijven wij hoe een bestuur via een geïntegreerde aanpak – die bestaat uit zes stappen – de regie kan pakken en tot een consistent geheel van eisen aan een uitbestedingspartner kan komen. Deze aanpak sluit aan bij de (beperkte) regelgeving op dit gebied.[1]

GEÏNTEGREERDE AANPAK

Het is verleidelijk om op allerlei signalen, vanuit actualiteiten, good practices of signalen van de toezichthouder ad hoc en geïsoleerd te reageren. Meestal is dit niet de beste aanpak en leidt het niet tot het gewenste resultaat. Vaak is het beter om pas op de plaats te maken en na te gaan wat het totale beeld is en hoe dit past binnen de organisatie van het pensioenfonds. De volgende drie vragen moeten daarbij altijd worden gesteld:

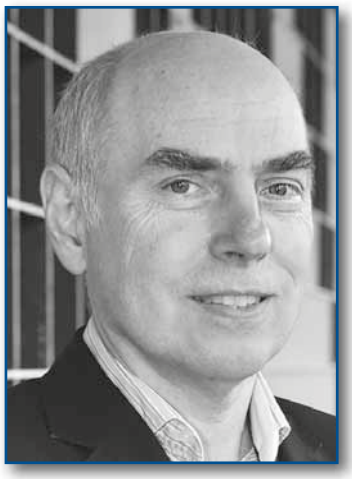
1. In hoeverre zijn de signalen relevant voor ons als pensioenfonds?
2. Beschik ik over alle relevante informatie?
3. Zijn de uit de signalen voortkomende aandachtspunten reeds verankerd in de organisatie?

Het antwoord op deze vragen leidt tot het inzicht of al dan niet actie nodig is. Om te bepalen welke acties nodig zijn, is het goed om systematisch na te gaan wat de antwoorden betekenen voor de eerste vier stappen om in de regie te komen:

1. het uitbestedingsbeleid van het pensioenfonds en de hieruit voortvloeiende concrete doelstellingen;
2. het risicobeeld en de gewenste beheersing hiervan;
3. de kaderstelling, oftewel de eisen die aan de uitbesteding worden gesteld;
4. de overeenkomst en de SLA met de desbetreffende uitbestedingspartner.

Wanneer deze stappen op een gedegen en systematische wijze worden doorlopen, heeft het bestuur zekerheid dat de eisen die aan de uitbestedingspartner worden gesteld, aansluiten bij de concreet geformuleerde doelstellingen van het pensioenfonds. Hierna gaan we nader in op de vier genoemde stappen. Via monitoring (stap 5) en evaluatie (stap 6) zal het bestuur vervolgens moeten nagaan of de uitbestedingspartner het bestaan en de werking van de afspraken kan aantonen.

> Veel fondsen blijven steken in algemeenheden; hierdoor ontbreekt vaak de link met de kaderstelling en met integraal risicomanagement



Marcel Baveco en Gerrit Liefers
Drs. ir. M.P.P. Baveco RE is directeur bij KoutersVanderMeer en drs. G. Liefers RA is senior consultant bij Willis Towers Watson

STAP 1. FORMULEER BELEID UITMONDEND IN CONCRETE DOELSTELLINGEN

Zoals gezegd zijn missie, visie en strategie van het pensioenfonds leidend voor de wensen en eisen die aan de uitvoering en uitbesteding worden gesteld. Het concreet vaststellen van doelstellingen op het gebied van uitbesteding is nodig om de risicobereidheid, de beheersing en het uitbestedingsbeleid op een consistente wijze vorm te geven. Veel fondsen blijven steken in algemeenheden; hierdoor ontbreekt vaak de link met de kaderstelling en met integraal risicomanagement (IRM). Ook wordt vaak vergeten dat het uitbestedingsbeleid moet zijn ingebed in de totale bestuurscyclus en dat het bestuur verantwoordelijk is voor de totale IT-keten van het pensioenfonds, ook voor het deel dat bijvoorbeeld is uitbesteed aan een of meer uitbestedingspartners. Veel fondsbesturen waren zich hier tot voor kort niet van bewust en beschikken niet over een IT-strategie en/of -beleid.

Als bestuur kun je sec een beleid formuleren. Integrale aanpak vanuit de basis draagt echter bij aan een gestructureerde beheersing van uitbestedingsrelaties. Daarom is het goed om even pas op de plaats te maken en de ontwikkelingen in perspectief te plaatsen, te beginnen vanuit de missie, visie en strategie. Van daaruit komt het bestuur tot (aanpassing van) een geïntegreerd uitbestedings- en IT-beleid, waarin een aantal concrete doelstellingen op het gebied van uitbesteding zijn opgenomen. Deze vormen de basis voor de verdere invulling van het IRM en de kaderstelling.

Hoe kan een fonds de doelstellingen concreet formuleren? Als eenvoudig voorbeeld nemen we de uitbesteding van de pensioenadministratie. Deze vormt de basis voor de communicatie van de opgebouwde pensioenen en is daarmee het 'kloppend hart' van het pensioenfonds. Foutieve communicatie tast de reputatie van een pensioenfonds snel aan en kan, onbedoeld, er ook toe leiden dat de integriteit van het pensioenfonds(bestuur) in twijfel wordt getrokken.

Voor de uitvoering van de pensioenadministratie kan de volgende algemene doelstelling zijn geformuleerd: 'Doel van de uitbesteding van de pensioenadministratie aan een professionele uitvoerder is constante kwaliteit van dienstverlening tegen een aanvaardbare (optimale) prijs.' Deze doelstelling moet verder worden geconcretiseerd om goed te kunnen bepalen welke risico's de doelstelling kunnen bedreigen. Dit werd in het verleden vaak vertaald als: de deelnemers-, uitkeringen- en financiële administraties moeten juist, volledig en tijdig worden uitgevoerd. Hiermee is echter nog niet de constante kwaliteit gewaarborgd, net zomin als de gewenste kostenbeheersing. Door de doelstellingen SMART te maken – Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdsgebonden – dragen ze bij aan een effectieve vertaling naar risico's, toleranties, beheersmaatregelen en afspraken met uitbestedingspartners.

STAP 2. BEPAAL DE RISICO'S DIE DE DOELSTELLINGEN KUNNEN BEDREIGEN

Nadat de doelstellingen verder zijn geoperationaliseerd in een uitbestedings- en IT-beleid, is het zaak te kijken naar de risico's die het realiseren van die doelstellingen kunnen bedreigen. Bij wijze van voorbeeld: de doelstelling 'constante kwaliteit van dienstverlening' kan worden bedreigd door het risico dat de hoogte van de uitkering niet juist, volledig of tijdig wordt vastgesteld, gecommuniceerd en uitbetaald. Dit risico kan verder worden uitgewerkt in subrisico's, zoals het risico dat de uitkeringen bij ingang en/of wijziging niet juist zijn vastgesteld. Bij de uitwerking is het ook van belang om de verschillende invalshoeken, zoals IT, medewerkers en procedures, in de beschouwing te betrekken. IT is tenslotte een middel dat bijdraagt aan de beheersing van de uitvoering. Wanneer de IT niet goed functioneert zal dit, net als het niet functioneren van medewerkers, invloed hebben op de constante kwaliteit van dienstverlening.

IT-risico

Een belangrijk IT-risico is het risico dat bedrijfsprocessen en informatievoorziening onvoldoende integer, niet continu of onvoldoende beveiligd worden ondersteund door IT. Dit risico kan op basis van het 4A's model van De Nederlandsche Bank als volgt worden uitgewerkt:

- het risico dat pensioeninformatie meer dan xx uur niet beschikbaar is (availability/beschikbaarheid);
- het risico dat pensioeninformatie in handen komt van onbevoegden (accessibility/vertrouwelijkheid);
- het risico dat de pensioeninformatie niet volledig en juist kan worden bewerkt en opgeslagen (accuracy/integriteit);
- het risico dat de IT niet aanpasbaar is aan toekomstige wetgeving (agility/aanpasbaarheid).

Wanneer de IT niet goed functioneert zal dit, net als het niet functioneren van medewerkers, invloed hebben op de constante kwaliteit van dienstverlening

STAP 3. KADERSTELLING ALS BASIS VOOR BEHEERSING

De kaderstelling is de basis voor de eisen die aan een uitbestedingspartner worden gesteld. Zonder kader-

1 Denk aan good practices van De Nederlandsche Bank (DNB) rond uitbesteding, IT, robuuste pensioenadministratie en de self assessment Informatiebeveiliging. Het toezicht is 'principle based' en met name gebaseerd op art. 143 PW.

stelling is onvoldoende duidelijk wat nodig is om in control te zijn en te blijven, kan geen goed selectietraject worden uitgevoerd en is er onvoldoende basis om voor het pensioenfonds de juiste contractuele afspraken te maken. Het bestuur moet de juiste informatie krijgen om de uitbestedingspartner te monitoren. Deze kaderstelling is geen statisch geheel, maar moet steeds opnieuw worden aangepast aan de 'veranderende werkelijkheid'. In de vastlegging van de kaderstelling is IT verweven in de eisen ten aanzien van uitbesteding.

Om vanuit de benoemde risico's op een verantwoorde wijze invulling te geven aan de kaderstelling, moet de risicobereidheid bekend zijn. Risicobereidheid beantwoordt de vraag: hoeveel risico is voor het fonds acceptabel, c.q. wenselijk? Het antwoord op deze vraag bepaalt mede de mate van beheersing van de risico's en daarmee de kaderstelling. Laten we het eerdere voorbeeld van de uitkeringsadministratie nog eens bezien. Tijdigheid is voor deze administratie belangrijker dan voor bijvoorbeeld de deelnemersadministratie. Immers, op de dag van de uitbetaling moet de uitkeringsadministratie volledig zijn bijgewerkt. Dit betekent dat er bij de uitkeringsadministratie meer

De kaderstelling is geen statisch geheel, maar moet steeds opnieuw worden aangepast aan de 'veranderende werkelijkheid'

nadruk op de beheersing van de tijdigheid zal liggen dan bij de deelnemersadministratie. Anders gezegd: de risicobereidheid en daarmee de tolerantie is met betrekking tot de tijdigheid van uitkeringen extreem laag. Daarom zullen daar ook extra eisen moeten worden gesteld aan onder andere de beschikbaarheid van de IT die het uitkeringsproces ondersteunt. Die beschikbaarheid wordt ondersteund door onder meer de volgende maatregelen:

- back-up van cruciale data; deze worden bijvoorbeeld online gemaakt naar een tweede rekencentrum;
- periodiciteit van testen van de uitwijkvoorziening van de uitvoerder; de gemaakte back-ups dienen dan succesvol te worden ingelezen en verwerkt;
- het stand-by hebben van een bancaire applicatie bij een andere bank om in geval van nood de betalingen te kunnen verrichten.

Om een constante kwaliteit aantoonbaar te waarborgen is het van groot belang dat ook kaders worden gesteld aan het IRM en het control framework van de uitvoerder(s). Hierbij is essentieel dat in de kaderstelling de klantspecifieke vereisten goed worden afgedekt en vastgelegd. Zorg er als bestuur voor dat de door de uitbestedingspartner gehanteerde toleranties of Key Risk Indicators (KRI's) minimaal gelijk zijn aan die van het bestuur. Dit wordt met name zichtbaar in de risicorapportage van de uitbestedingspartner. Hierbij valt onder meer te denken aan:

- eisen met betrekking tot de scope van de ISAE3402/3000 type 2 verklaringen: deze worden jaarlijks verstrekt door de uitvoerder en hebben betrekking op opzet, bestaan en werking van belangrijke beheersmaatregelen, waaronder de IT;
- de scope van de Service Level rapportages: deze worden maandelijks of per kwartaal verstrekt door de uitbestedingspartner;
- andere periodieke door de uitbestedingspartner verstrekte risicorapportages, bijvoorbeeld over de beheersing van risico's bij grote veranderingstrajecten met een IT-component of actuele thema's als de beheersing van cybersecurity;
- rapportages van tweedelijns audits door de uitbestedingspartner.

STAP 4. OVEREENKOMST EN SLA MET UITBESTEDINGSPARTNER

De kaderstelling vormt de basis voor de aan de uitbestedingspartner te stellen eisen en de afspraken die met hem moeten worden gemaakt. Deze moeten zo veel mogelijk SMART worden uitgewerkt in de overeenkomst en in de Service Level Agreement (SLA) met de uitbestedingspartner. Hierbij valt te denken aan:

- de overeengekomen eisen aan het control en risk framework van de uitbestedingspartner en hoe deze bewijst dat deze continu functioneren (denk aan de hiervoor genoemde verklaringen);
- de wijze waarop de uitbestedingspartner het bestuur in staat stelt om op alle relevante gebieden in control te zijn (denk aan eerdergenoemde ISAE-verklaringen, risicorapportages, rapportages omtrent SIRA etc.);
- clausules over de mogelijkheid voor (vroegtijdige) beëindiging of aanpassing tijdens de looptijd;
- escalatieprocedure voor het moment waarop de services niet volgens de afgesproken levels worden geleverd.

De SLA vormt de basis voor het prestatiemanagement van de uitbestedingspartner. Per (deel)proces wordt het in stap 3 opgestelde kader vertaald naar Key Performance Indicators (KPI's) en Key Risk Indicators (KRI's). Deze vormen de basis voor de monitoring. Het hiervoor als voorbeeld genoemde kader voor de uitkeringsadministratie zal leiden tot een aantal gedetailleerde serviceafspraken.

STAP 5. MONITORING

Het bestuur kan op papier goede afspraken maken met de uitbestedingspartners, maar het moet ook nagaan of ze worden nagekomen. Uiteindelijk staat of valt een goede monitoring met gedegen rapportages die de aantoonbare werking van de gemaakte afspraken inzichtelijk maken. Deze rapportages dienen door het pensioenfondsbestuur te worden beoordeeld op de voor het pensioenfonds essentiële zaken. De vastlegging van deze beoordeling is belangrijk, omdat ze kan worden gebruikt voor verdere bijsturing en verantwoording, zowel intern en extern als voor de evaluatie.

Voor deze verantwoordingsrapportage is een risicogebaseerde aanpak het uitgangspunt: voor kritieke processen moet in het algemeen de rapportagefrequentie hoger zijn en de aard van de rapportage meeromvattender dan voor de minder kritieke processen. Dit heeft zich als het goed is al in stap 4 vertaald naar de nodige KRI's.

Uiteindelijk staat of valt een goede monitoring met gedegen rapportages die de aantoonbare werking van de gemaakte afspraken inzichtelijk maken

Nogal eens wordt door de uitbestedingspartner alleen in algemene zin gerapporteerd over de beheersing. Het pensioenfonds zal dan aanvullende verantwoordingsinformatie moeten opvragen om te bepalen of de uitbestedingspartner aan de eisen van het fonds voldoet. In toenemende mate worden jaarlijks ISAE3402- en ISAE3000-verklaringen door de uitbestedingspartner verstrekt. Dit is een positieve ontwikkeling, omdat de uitbestedingspartner hierbij verantwoording aflegt over de werking van beheersmaatregelen (niet-financieel en financieel) binnen een groot deel van de uitbestede processen. Het fonds zal bij deze verklaringen moeten beoordelen of de scope past bij de gemaakte afspraken, of het het type 2 verklaringen zijn – wordt over de werking gerapporteerd? – of de verklaringen schoon zijn en of er mogelijk beperkingen zijn waarover het bestuur in overleg zal moeten treden met de uitbestedingspartner.

STAP 6. EVALUATIE

Periodiek zal het pensioenfonds de geleverde service moeten evalueren. Dit kan op basis van de Service Level rapportages en de andere verantwoordingsrapportages, zoals de ISAE3402 of ISAE3000-verklaringen, en zal vaak steunen op de uitkomsten van de monitoring. In de evaluatie moet ook de toekomstbestendigheid van de uitbestedingspartner worden meegenomen. Hierbij valt te denken aan zaken als:

- past de partner nog bij de eigen toekomstvisie;
- de uitbestedingspartner lijdt grote verliezen, hoelang kan deze dit nog volhouden;
- de uitbestedingspartner heeft vanwege zijn beperkte omvang onvoldoende mogelijkheden om te investeren;
- het IT-platform is verouderd en kan niet of alleen tegen hoge kosten worden aangepast aan nieuwe wettelijke vereisten;
- de softwareleverancier van de uitbestedingspartner stopt met onderhoud van de belangrijkste onderdelen van het IT-platform.

De evaluatie kan naast contractuele wijzigingen of beëindiging ook leiden tot herijking van het uitbestedings- en IT-beleid van het fonds en het verder aanscherpen van de eisen aan de uitbestedingspartner en de verantwoordingsrapportage. Wanneer uit de evaluatie blijkt dat de uitbestedingspartner (mogelijk)

IT risicobereidheid en haar invloed op kaderstelling en SLA

Voor het vaststellen van de risicobereidheid waarbij voor de IT het 4A's model van DNB wordt gehanteerd zal de classificatie per A (of: IT-element) moeten worden bepaald. Deze classificatie geeft het belang aan van dit element voor de bedrijfsvoering van het fonds, bijvoorbeeld op een schaal van 0 tot 3, waarbij 0 = laag belang en 3 = groot belang. Als voorbeeld wordt hier het proces van de pensioenadministratie beoordeeld. Het pensioenfonds bepaalt op basis van een risicoanalyse (stap 2) de volgende classificatie voor de applicaties die dit proces ondersteunen. Hierbij geven de vetgedrukte kwalificaties de keuzes van het pensioenfonds weer – in dit voorbeeld is dit alleen uitgewerkt voor availability en accessibility.

IT-element	classificatie			
	0	1	2	3
availability	niet nodig	belangrijk	noodzakelijk	**essentieel**
accessibility	openbaar	bedrijfsvertrouwelijk	**vertrouwelijk**	geheim
accuracy	..	..	..	..
agility	..	..	..	..

Uit deze classificatie blijkt dat de beschikbaarheid van de applicatie voor de pensioenadministratie 'essentieel' is: hieraan worden door het fonds de hoogste eisen gesteld, die worden neergelegd in de kaderstelling (stap 3) en bij uitbesteding ook in de SLA (stap 4).
Vervolgens zal moeten worden bekeken welke beheersmaatregelen er daadwerkelijk al door fonds of uitbestedingspartij zijn getroffen om dit brutorisico te mitigeren: het nettorisico zal worden bepaald. Als blijkt dat de huidige maatregelen onvoldoende zijn, moeten er aanvullende maatregelen worden getroffen, net zolang tot de kans en impact binnen de gestelde grenswaarde ligt. Deze totale set van beheersmaatregelen vormt de basis voor de afspraken die in de SLA moeten worden vastgelegd en waarover dient te worden gerapporteerd.

niet meer past bij het fonds, kan worden gestart met een marktverkenning, die kan leiden tot de overgang naar een andere uitbestedingspartner. Hiermee is de cirkel weer rond.

TEN SLOTTE

In dit artikel stelden we vast dat het uitbestedingsbeleid, inclusief het IT-beleid, moet zijn ingebed in de bestuurscyclus van het pensioenfonds omdat de uitbesteding de gestelde doelen moet dienen. Dit beleid moet uitmonden in concrete doelstellingen; alleen wanneer deze voldoende concreet zijn kunnen de risico's die de doelstellingen kunnen bedreigen, waaronder IT-risico's, goed in kaart worden gebracht. Op grond van de risicobereidheid kunnen vervolgens de vereiste beheersmaatregelen worden benoemd, die hun weerslag vinden in de kaderstelling. Pas als dit traject goed is vormgegeven, kan worden vastgesteld of de juiste uitbestedingspartner(s) is/zijn geselecteerd en welke afspraken in de Service Level Agreement moeten worden opgenomen. Deze dienen als input voor de SLA-rapportages van de uitbestedingspartners en als startpunt voor de monitoring en evaluatie voor de fondsbesturen. Betrek in de evaluatie zeker ook de toekomstvastheid, ook op IT-gebied, van de uitvoerder. Als dit proces goed is vormgegeven, is het bestuur volledig in control.

boeken

Memo Financiële planning – Het (nieuw) huwelijksvermogensrecht

Mr. Theo Hoogwout en Ramón Wernsen MFP, FFP, CFP

Dit boek beschrijft het – per 1 januari 2018 vernieuwde – huwelijksvermogensrecht en de invloed van relatievormen en gebeurtenissen op de financiële planning. In de tekst treft u vele verwijzingen aan naar relevante wetsartikelen en rechtspraak.
Onvoorziene levensgebeurtenissen, zoals scheiding en vroegtijdig overlijden, kunnen grootschalige gevolgen hebben voor de financiële positie van een of beide partners. Memo Financiële Planning – Het (nieuw) huwelijksvermogensrecht geeft inzicht in de civiel- en fiscaalrechtelijke gevolgen van dergelijke gebeurtenissen voor samenlevers, gehuwden en geregistreerd partners, waarbij ook de sociale-zekerheidsaspecten niet onbelicht blijven. De uitgave beschrijft wat men kan regelen voor het samenleven of huwelijk en hoe na overlijden de partner goed verzorgd kan achterblijven.
Steeds meer beroepsgroepen tonen belangstelling voor financiële planning. Daarom is deze uitgave niet alleen interessant voor de financieel planner, maar ook voor de accountant, belastingadviseur, estate planner, private banker, echtscheidingsadviseur, hypotheekadviseur en beleggingsadviseur.

Kluwer, Deventer 2019
Omvang: 226 pag.'s
Prijs: € 35,95 (incl. btw), abt. € 32,35 (incl. btw)
ISBN 9789013151145