Bert Keuter

LUIK 1
BASISKENNIS
PENSIOEN

Hoe gaat pensioenuitvoerder TKP in de praktijk om met het ISAE 3402-assurancerapport? Hoe beoordeelt TKP met een eigen framework het rapport van de uitbestedingspartners en welke rol kan de interne auditor hebben bij het totstandkomen van de eigen assurancerapportage en het beoordelen van assurancerapportages?

Meer halen uit **assurancerapporten**

In Nederland wordt een pensioen (dus niet de AOW) veelal verzorgd door pensioenuitvoerders zoals pensioenfondsen, verzekeraars, premiepensioeninstellingen (PPI's) en in de nabije toekomst ook door de nieuwe algemeen pensioenfondsen (APF'en). In veel gevallen hebben deze organisaties werkzaamheden uitbesteed aan partners zoals pensioenuitvoeringsorganisaties (puo's) zoals TKP en vermogensbeheerders. Een bekend voorbeeld van deze uitbesteding is het pensioenfonds ABP dat de administratie heeft uitbesteed aan de pensioenuitvoeringsorganisatie APG.

TKP Pensioen

TKP Pensioen (TKP) is een professionele pensioenuitvoeringsorganisatie met meer dan 25 jaar ervaring in dienstverlening op het gebied van pensioenuitvoering en -advisering. TKP is een 100% dochter van Aegon en werkt met ongeveer 750 medewerkers voor ruim 30 klanten waaronder ondernemingspensioenfondsen, bedrijfstakpensioenfondsen, PPI's en een Algemeen Pensioen Fonds (APF).

TKP besteedt op haar beurt processen uit aan bijvoorbeeld een creditmanager, een human resource service provider en enkele andere specialistische bedrijven, de 'onderuitbesteders'. Om het geheel aan uitbestedingen voor de lezer overzichtelijk te houden is in dit artikel gekozen voor de termen opdrachtgever, aannemer en onderaannemer. *Figuur 1* geeft een grafische weergave van de keten van uitbestedingen weer.

Standaard

Een veelgebruikte assurancevorm bij uitbesteding is de ISAE 3402-standaard.[1] Deze standaard maakt het voor een serviceorganisatie mogelijk om een assurancerapport te overhandigen dat uitbesteders kunnen gebruiken om zekerheid te krijgen over de betrouwbaarheid van de service. TKP stelt als pensioensuitvoeringsorganisatie (aannemer) een dergelijk rapport op ten behoeve van de pensioenuitvoerder (opdrachtgever). Daarnaast maakt TKP (als opdrachtgever) gebruik van assurancerapporten van onderaannemers (opdrachtnemer). In het figuur is dit schematisch weergegeven.

Het rapport kan eventueel, indien adequaat ingericht, breder worden gebruikt. In geval van onderuitbesteding blijft de opdrachtgever geheel verantwoordelijk voor het hele proces en is het noodzakelijk assurance te krijgen over de beheersing van de werkzaamheden die worden uitgevoerd. Er moet

Figuur 1. Uitbestedingspartners, opdrachtgever, aannemer en onderaannemer

dan worden beoordeeld of het assurancerapport inzicht geeft in de beheersing van onderaannemers.

Beoordeling assurancerapportages

Als onderdeel van het TKP framework 'Beheersing uitbesteding' beoordeelt TKP assurancerapportages van de onderaannemers. Jaarlijks beoordeelt TKP ongeveer tien ISAE 3402 type II-rapporten. TKP beoordeelt onder andere rapporten van ICT-dienstverleners, vermogensbeheerders, een creditmanager en een hr service provider.

Het onderzoek wordt uitgevoerd in twee fasen, een deskresearch gevolgd door onderzoek ter plaatse. Het assurancerapport wordt getoetst aan de volgende beoordelingscriteria: scope, dekking, type, reikwijdte, diepgang, relevante wijzigingen, bevindingen & impact, verklaring van het management, verklaring van de accountant, beheersing uitbesteding, privacy en opvolging van de bevindingen. De resultaten van het deskresearch zijn input voor het onderzoek ter plaatse.

Beoordelingscriteria uit framework

Het is belangrijk om vast te stellen dat de dienstverlening die is uitbesteed door klanten in scope is van het rapport. Het kan namelijk zijn dat de processen die een organisatie heeft uitbesteed niet of onvoldoende in scope zijn geweest van het onderzoek.

Dekking

De dekking van het rapport geeft informatie over de periode waar de assurance over gaat. Geeft het rapport wel zekerheid over de periode waarover zekerheid gezocht wordt? Mocht dat niet het geval zijn dan is het belangrijk te bepalen welke aanvullende zekerheid de uitbestedingspartner kan verschaffen. Deze kan onder andere bestaan uit aanvullende onderzoeken maar ook uit zogenaamd 'bridge letters' van de serviceorganisatie. Bij dit laatste is het belangrijk na te vragen of deze verklaring onderbouwd is door een onderzoek van een interne auditfunctie of dat het gaat om een ongetoetste verklaring.

De ISAE 3402-standaard kent twee typen. Type I geeft zekerheid over opzet en bestaan van de beheersmaatregelen. Type I wordt meestal gebruikt als een voorbereidende fase voor een type II rapport. Het type II-rapport geeft naast zekerheid over opzet en bestaan ook zekerheid over de werking van de beheersmaatregelen gedurende een bepaalde periode. Type II geeft de zekerheid die vaak gezocht wordt. In de praktijk komt TKP type I-verklaringen alleen maar tegen als een dienstverlener net gestart is met het uitbrengen van een ISAE 3402-rapport. Het type I-rapport wordt meestal binnen een half jaar of jaar gevolgd door een jaarlijks type II-rapport.

Reikwijdte

Om de reikwijdte van het rapport te beoordelen kunnen

verschillende methoden gebruikt worden. Een methode die TKP gebruikt is het matchen van de service level agreement (SLA) met het assurancerapport. In deze matching worden de afspraken uit de SLA vergeleken met de beheersmaatregelen uit het assurancerapport. Het resultaat van deze matching is een overzicht dat soms nog 'witte vlekken' (relevante afspraken die niet worden afgedekt) kent. Deze witte vlekken kunnen daarna besproken worden met de eigen organisatie, maar ook met de serviceorganisatie. TKP heeft goede ervaringen met het expliciet bespreken van witte vlekken. In een aantal gevallen heeft dit ertoe geleid dat rapporten van uitbestedingspartner zijn aangepast om zo te komen tot een waardevoller rapport voor TKP en ook voor andere klanten.
Overigens is de praktijk dat de SLA en het assurancerapport nooit 100% matchen. Dit hoeft niet onoverkomelijk te zijn zolang de risicovolle onderdelen van de uitbesteding geen witte vlek zijn.

Diepgang
Bij het beoordelen van diepgang van een assurancerapport wordt onderzocht of de beschreven processen en de beheersmaatregelen voldoende zijn beschreven; is er een goede mix van de verschillende soorten beheersmaatregelen?

Relevante wijzigingen
Het hoofdstuk relevante wijzigingen in het assurancerapport geeft inzicht in welke processen zijn toegevoegd, verwijderd of aangepast. Dit geeft een goed inzicht in de ontwikkelingen van beheersmaatregelen en de scope.

Bevindingen
Als een assurancerapport bevindingen bevat dan hebben deze meestal impact. Het is belangrijk om te onderzoeken wat de relevantie is van deze bevindingen voor de beheersing van de dienstverlening die is uitbesteed. Dit kan reden zijn om zelf aanvullende controles uit te (laten) voeren.

Als aan alle controledoelstellingen is voldaan geeft de accountant een goedkeurende verklaring. In sommige gevallen geeft de accountant een verklaring met beperking. Mocht hiervan sprake zijn dan kan de impact groot zijn, omdat een deel van de gezochte zekerheid niet kan worden gegeven. Het is belangrijk te weten hoe de uitbestedingspartner hiermee omgaat en welke stappen worden genomen om de interne beheersing te versterken. TKP heeft goede ervaringen met het expliciet bespreken van de hiervoor genoemde punten. Het biedt de mogelijkheid om eventuele problemen tijdig te bespreken en te adresseren.
De beschreven werkwijze kan ook worden gebruikt bij andersoortige assuranceonderzoeken. Het rapport is mogelijk bruikbaar bij beheersing van IT-risico's en informatiebeveiliging.[2,3] TKP heeft goede ervaringen met deze manier van systematisch het ISAE 3402-rapport te beoordelen.

De rol van auditor bij pensioenuitvoering
De plaats van de interne auditor is afhankelijk van de organisatie. Verzekeraars, pensioenuitvoeringsorganisaties en vermogensbeheerders beschikken meestal over een interne auditfunctie. Pensioenfondsen, PPI's en APF'en beschikken vaak niet over een permanente interne auditfunctie.
Ongeacht de formele plaats van de interne auditor in de organisatie kan de auditor verschillende aspecten van interne beheersing van de organisatie toetsen aan de hand van een assurancerapport en dit ook gebruiken bij andere werkzaamheden. Voorbeelden hiervan zijn werkzaamheden die onderdeel zijn van het internal auditjaarplan maar ook audits die deel uitmaken van een jaarrekening controle, SOx-controles of ISAE 3402 audits. Daarnaast kan de interne auditor gevraagd worden onderzoek te doen naar de interne beheersing van de uitbestedingspartner.

Periodieke herhaling en een blik op de toekomst
TKP heeft ervaren dat het jaarlijks herhalen van de beoordeling van het assurancerapport van de uitbestedingspartners de organisatie veel inzicht geeft in de beheersing van de processen die zijn uitbesteed. Dit beoordelen is onderdeel van de beheersing van de uitbesteding en kan helpen om ten aanzien van de uitbestede processen aantoonbaar in control te zijn. Ontwikkelingen op het gebied van interne beheersing en het geven van zekerheid hierover volgen elkaar in snel tempo op. Drivers hiervoor zijn strengere vereisten voortkomend uit wet- en regelgeving en de vraag naar continue zekerheid. <<

Het herhalen van de beoordeling geeft veel inzicht in de beheersing van de processen

Noten
1. ISAE3402 - http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf
2. Beheersing IT risico - http://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-pensioenen/nieuwsbrief-pensioenen-juli-2015/dnb323390.jsp
3. Toetsingskader Informatiebeveiliging - http://www.toezicht.dnb.nl/3/50-203304.jsp

Bert Keuter is manager Operational Risk Management & Compliance bij TKP. Hij bekleedde bij verschillende organisaties rollen als security manager, operational risk manager en business continuity manager.