Volwassenheidsniveau risicobeheer

Pensioenfondsen in Nederland

KPMG Advisory N.V.

—

Juni 2021

Inhoudsopgave

Aanleiding

Met de grootste pensioenhervorming in jaren voor de deur zal risicobeheer de komende jaren prominent op de bestuursagenda staan. Hoe staat het met de volwassenheid van de Nederlandse pensioenfondsen op dat gebied?

Mede naar aanleiding van de introductie van IORP II en de verhoogde aandacht van de toezichthouder is de professionalisering van het risicobeheer in de Nederlandse pensioensector de laatste jaren in een stroomversnelling geraakt. Met de overgang naar het nieuwe pensioenstelsel, de grootste pensioenhervorming in jaren, zal het risicobeheer de komende jaren prominent op de bestuursagenda blijven staan. Hierbij komt de ambitie vanuit de fondsen steeds vaker expliciet naar voren om het risicobeheer meer integraal in te richten en de opzet, het bestaan en vooral de werking aantoonbaar te maken.
Om inzicht te geven in de huidige status van het volwassenheidsniveau van het risicomanagement in de pensioensector, heeft KPMG Advisory N.V. een benchmarkstudie uitgevoerd onder dertien Nederlandse pensioenfondsen, welke samen circa 15% van de markt vertegenwoordigen op basis van het belegd vermogen. Middels dit rapport presenteren wij u graag de uitkomsten van de benchmark.

Veronique de Boer-Achmad en Bianca Meijer

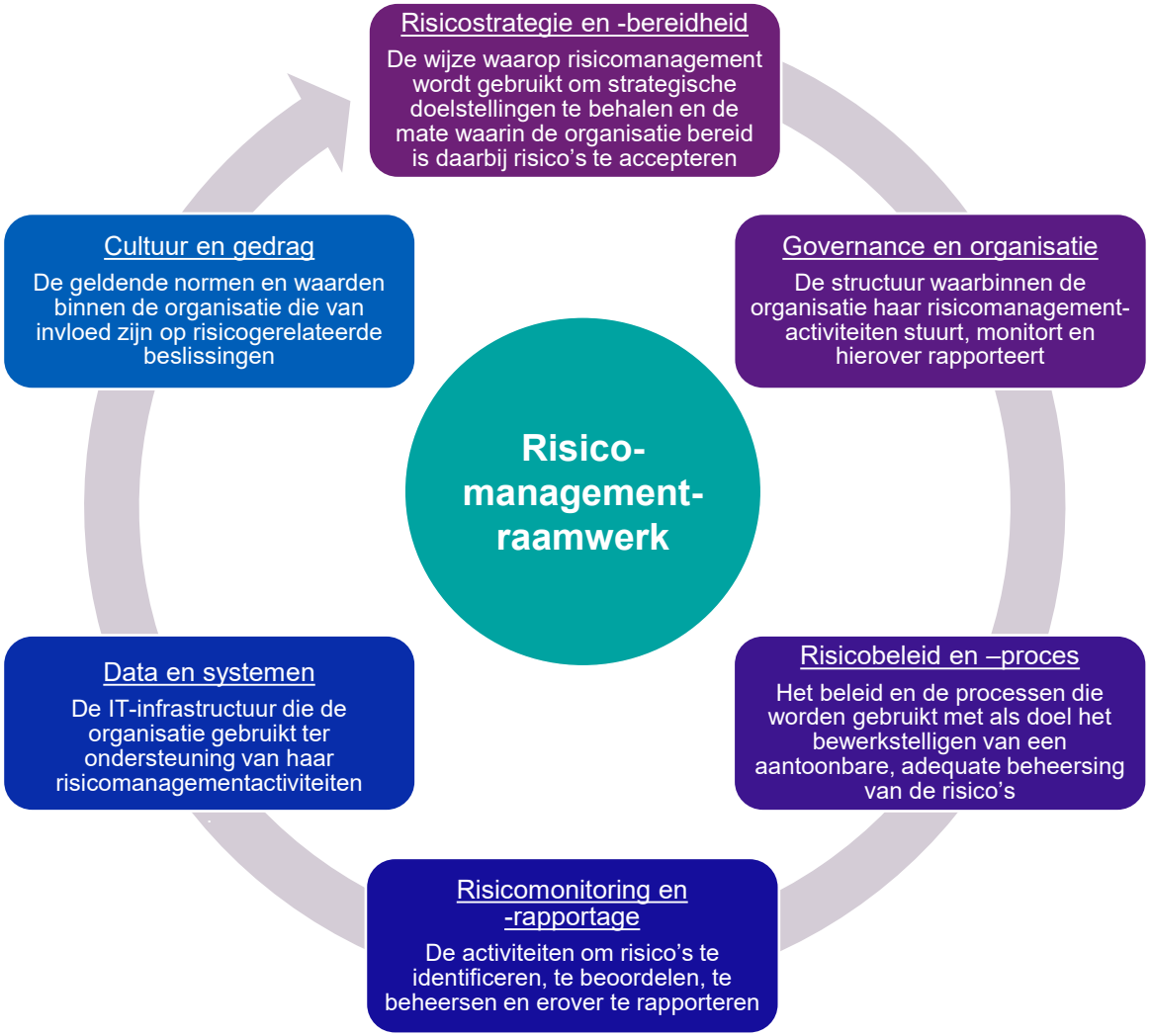
KPMG

Risicomanagement-raamwerk

Het raamwerk

Het risicomanagementraamwerk, of het risicobeheerraamwerk, dat in de praktijk door veel pensioenfondsen wordt toegepast, kan worden onderverdeeld in verschillende elementen zoals hiernaast weergegeven.

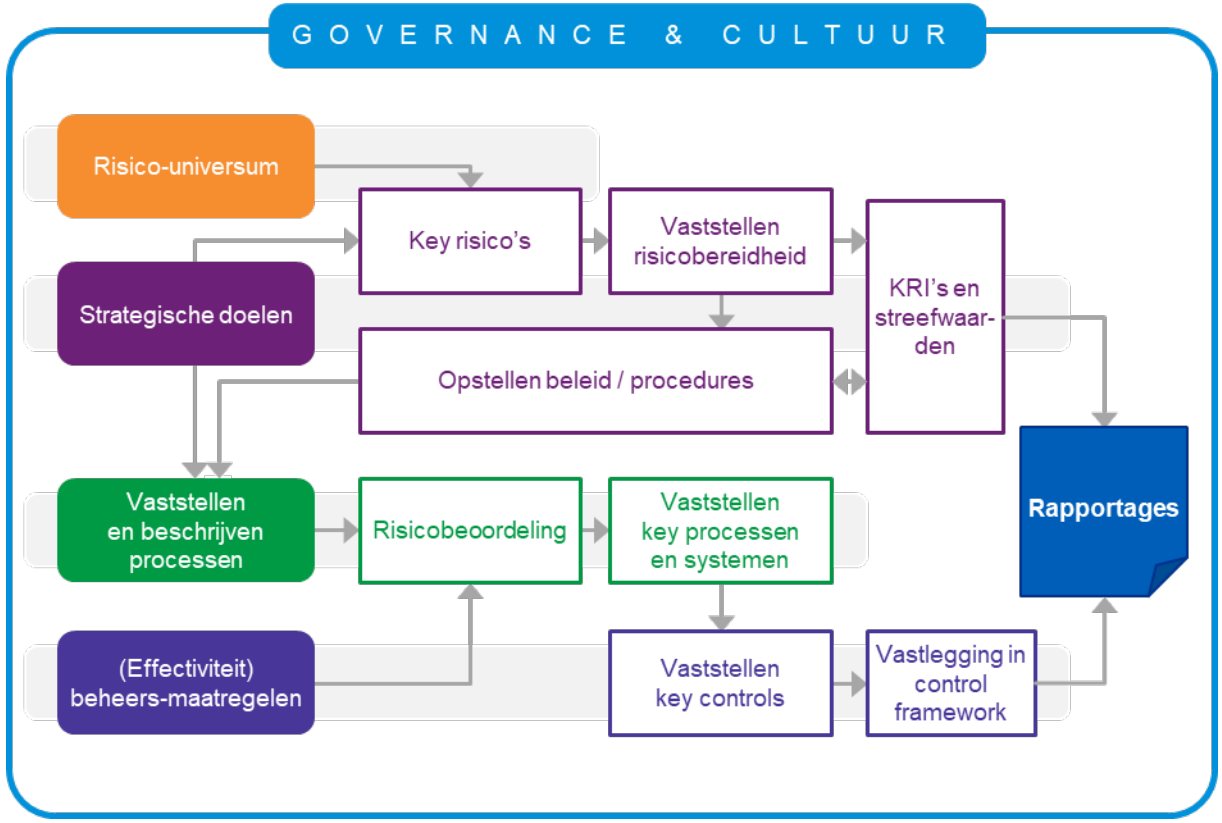
Dit raamwerk vormt de basis voor deze benchmark. Het raamwerk sluit aan bij het COSO ERM 2017*-model en legt daarmee de nadruk op de wisselwerking tussen strategie, prestaties en risico's.



*Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management (ERM) met in 2017 de update 'Integrating with Strategy and Performance'

Samenhang binnen het raamwerk

De verschillende elementen binnen het raamwerk zijn veelal bekend. Meer aandacht kan nog gegeven worden aan de samenhang tussen de verschillende elementen onderling.



KPMG

Onderzoeks-methode

Toelichting onderzoeksmethode

Deze benchmarkstudie is gebaseerd op interviews met risicobeheer(sleutel)-functionarissen van pensioenfondsen in Nederland. Aan het onderzoek hebben dertien pensioenfondsen deelgenomen welke samen circa 15% van de markt vertegenwoordigen, gemeten op basis van het belegd vermogen.

Het risicomanagementraamwerk dat in de praktijk door pensioenfondsen wordt toegepast kan worden onderverdeeld in verschillende elementen zoals hiervoor is toegelicht. Omdat de volwassenheid per element van het raamwerk binnen een pensioenfonds sterk kan verschillen, hebben wij, op basis van de gehouden interviews, elk van de deelnemende pensioenfondsen per element een score van 1 tot 5 toegekend. Het daarbij gehanteerde beoordelingskader wordt op de volgende pagina's toegelicht. Welke score als voldoende gezien mag worden is mede afhankelijk van de situatie en de ambitie van het pensioenfonds zelf, waarbij de toezichthouder in het algemeen impliciet een score van minimaal 3 voor het raamwerk als geheel verwacht.

Noot: In dit onderzoek zijn overigens geen scores toegekend op het element 'Cultuur en gedrag'. Het afnemen van een interview met slechts één of twee betrokkenen bij het pensioenfonds geeft op dit element onzes inziens een te beperkte weergave.

Toelichting beoordelingskader (1/2)

In dit onderzoek is gebruikgemaakt van een vijfpuntsschaal voor de beoordeling van het volwassenheidsniveau. Onderstaand wordt toegelicht welke eisen aan elke score zijn gesteld ter toekenning van de betreffende score. Deze vijfpuntsschaal is gebaseerd op de definities van volwassenheid zoals deze worden gehanteerd door DNB. In de bijlage is een nadere uitwerking van dit beoordelingskader, per element van het risicomanagementraamwerk, opgenomen.

01

Initieel

Governancevereisten voor een formeel risicomanagementkader zijn niet of nauwelijks aanwezig. De risicomanagementprocessen en -kaders zijn niet volledig gedocumenteerd, inconsistent en/of onduidelijk. Risicomanagementactiviteiten zijn niet (voldoende) afgestemd op de bedrijfsstrategie en de uitvoering van risicomanagementactiviteiten is afhankelijk van individuen.
De risicomanagementcyclus wordt in beperkte mate doorlopen.

02

Reproduceerbaar en informeel

Het pensioenfonds voldoet aan de minimale verwachtingen van interne en externe belanghebbenden ten aanzien van risicomanagementactiviteiten. Enkele risicomanagementactiviteiten zijn vastgesteld en gedocumenteerd en zijn (in elk geval deels) in lijn met de strategie. Er is een beperkte focus op opkomende risico's en/of samenhang tussen risico's. Risicobeleid en -processen zijn op hoofdlijnen gedocumenteerd, maar niet integraal vastgesteld. Beheersmaatregelen zijn genomen, maar niet formeel vastgelegd en de effectiviteit wordt niet standaard integraal beoordeeld.

Toelichting beoordelingskader (2/2)

Gedefinieerd

Het bestuur vertrouwt steeds meer op een effectieve beheersing van risico's middels aantoonbare inspanningen. De risicobereidheid is integraal vastgesteld en waar mogelijk middels relevante KRI's, doorvertaald naar toleranties en limieten. Risicobeheeractiviteiten zijn gericht op het behalen van de strategie. Het risicomanagementproces wordt periodiek geëvalueerd, maar dit is nog niet altijd aantoonbaar.

Beheerst en meetbaar

De risicobeheersmaatregelen zijn geïntegreerd en gecoördineerd en de doelstellingen voor risicobeheer zijn consistent in lijn met de strategie van het fonds. De risicomanagementcyclus wordt aantoonbaar periodiek doorlopen en mitigerende maatregelen worden periodiek aantoonbaar integraal geëvalueerd. De uitkomst van de evaluatie geeft aantoonbaar aanleiding tot aanpassingen. Er wordt waar relevant infrastructuur gebruikt voor ondernemingsbrede risicometing, -beheersing en -rapportage.

Continu verbeteren

De risicomanagementactiviteiten zijn volledig ingebed in strategische planning en de dagelijkse besluitvorming. Er is een goed werkend systeem om het bestuur vroegtijdig te waarschuwen en op de hoogte te stellen van risico's buiten de vastgestelde toleranties en limieten. Risicobeheer dient als bron van concurrentievoordeel.

KPMG

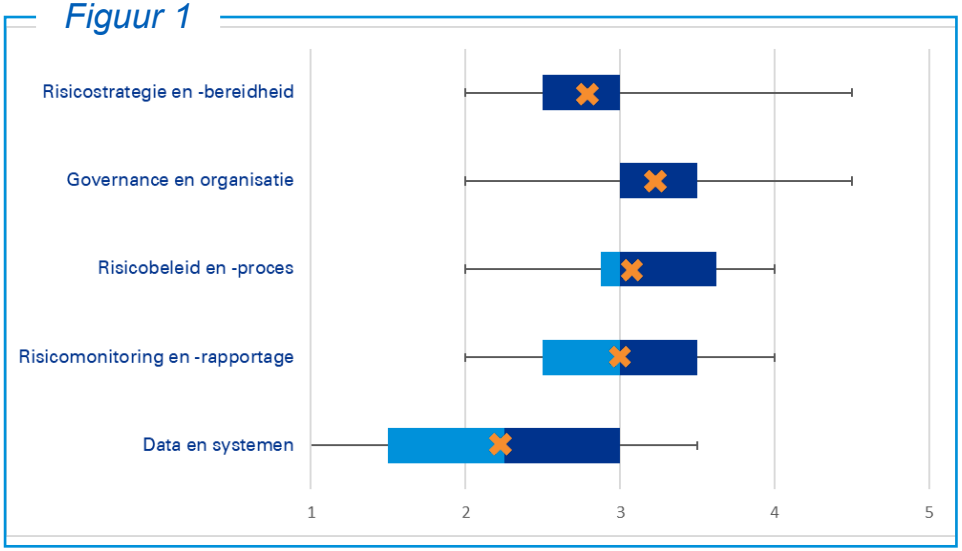
Resultaten

Uitkomst benchmarkonderzoek

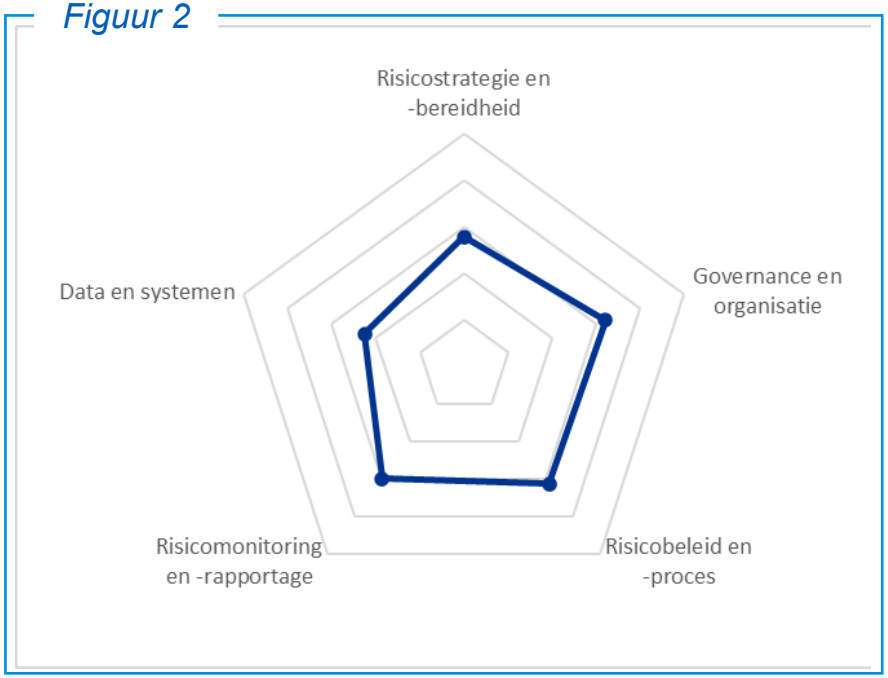
De pensioenfondsen opgenomen in deze benchmark scoren gemiddeld, over alle elementen heen, een 2,9. Dit betekent dat de pensioenfondsen gemiddeld genomen als 'volwassen' mogen worden beschouwd, maar voor de onderdelen van het risicobeheer die lager dan een 3 scoren nog verder moeten ontwikkelen.

Figuur 1 geeft de boxplots per element van het raamwerk weer. Uit deze boxplots kan informatie over de verdeling van de scores tussen de verschillende deelnemende fondsen worden gehaald. In figuur 2 is een spiderweb weergegeven. Hiermee is inzichtelijk gemaakt hoe de pensioenfondsen gemiddeld gezien op de verschillende elementen van het risicomanagementraamwerk hebben gescoord. Te zien is dat de gemiddelde score op alle elementen rond 3 ligt, met uitzondering van de score op het element ‘Data en systemen’. Op de volgende pagina’s wordt per element een toelichting gegeven.

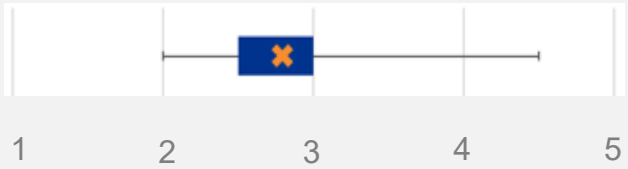
Figuur 1



Figuur 2



Risicostrategie en -bereidheid



Uitkomsten en bijzonderheden

Op het element ‘Risicostrategie en -bereidheid’ zijn scores tussen 2 en 4,5 toebedeeld. De meeste scores liggen tussen 2,5 en 3. De mate van spreiding op dit element is zeer beperkt.

Toelichting

‘Risicostrategie en -bereidheid’ hebben betrekking op de wijze waarop risicomanagement wordt gebruikt om strategische en overige doelstellingen te behalen.
De risicobereidheid geeft de bandbreedte aan waarbinnen het pensioenfonds bereid is tot het nemen van risico’s. Dit kan zowel in kwalitatieve als in kwantitatieve termen of een combinatie daarvan zijn geformuleerd.

Resultaten

Fondsen scoren gemiddeld 2,9 van de 5 punten op het element ‘Risicostrategie en -bereidheid’. De risicostrategie en -bereidheid zijn over het algemeen geheel vastgesteld. Doelen voor het risicomanagement zijn geformuleerd en een link met de strategie wordt door veel fondsen al grotendeels gemaakt.

Waar de risicobereidheid voor financiële risico’s vaak integraal is vastgesteld en vertaald naar meetbare KRI’s, kan er ten aanzien van de uitwerking van de risicobereidheid voor niet-financiële risico’s vaak nog een stap worden gezet. Denk hierbij aan (1) het opstellen van KRI’s met bijbehorende streef- en tolerantiewaarden en (2) actief hierop sturen.

Veel pensioenfondsen besteden cruciale processen uit. Algemeen aandachtspunt is dat ook voor de uitbestede processen geldt dat het fonds zélf ‘in control’ dient te blijven over de hieruit voortvloeiende risico’s. Dit vereist periodieke risicoanalyses door het fonds zelf en heldere afspraken over onder andere de periodieke rapportage van de uitbestedingspartijen, zodat het actuele risicoprofiel kan worden vergeleken met de risicobereidheid van het fonds.

Governance en organisatie

Uitkomsten en bijzonderheden

Op het element ‘Governance en organisatie’ zijn scores tussen 2 en 4,5 toebedeeld. De meeste scores liggen tussen 3 en 3,5. De mate van spreiding op dit element is zeer beperkt.

Toelichting

Onder ‘Governance en organisatie’ wordt de structuur verstaan waarbinnen het pensioenfonds zijn risicomanagementactiviteiten stuurt, monitort en hierover rapporteert. Deze organisatiestructuur omvat duidelijk omschreven taken en verantwoordelijkheden, inclusief beslissingsbevoegdheden en rapportagelijnen.

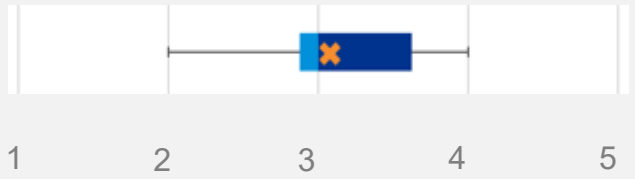
Resultaten

Op dit element wordt gemiddeld 3,1 van de 5 punten gescoord. De functies van het veel gebruikte ‘three lines model’* zijn formeel ingericht. De rollen en verantwoordelijkheden zijn gedocumenteerd, maar nog niet altijd integraal vastgesteld. Risicomanagement maakt in het algemeen aantoonbaar deel uit van de besluitvorming. De benodigde kennis en competenties voor goed risicomanagement zijn impliciet bekend, maar niet altijd vastgesteld.

Bij een meerderheid van de deelnemende fondsen kan de scheiding tussen de verschillende ‘lijnen’ uit het ‘three lines model’ nog scherper worden neergezet. Als verantwoordelijkheden door elkaar heen lopen, kan de onafhankelijkheid van de tweede lijn in het geding komen. Daarnaast valt op dat kennis van specifieke risico’s (zoals IT- en ESG-risico’s) niet altijd in voldoende mate aanwezig is; dit geldt voor zowel de eerste als de tweede lijn.

**Het ‘three lines model’ wordt ook wel ‘three lines of defence’- of ‘three lines of responsibilities’-model genoemd*

Risicobeleid en -proces



Uitkomsten en bijzonderheden

Op het element ‘Risicobeleid en -proces’ zijn scores tussen 2 en 4 toebedeeld. De meeste scores liggen tussen 2,5 en 3,5.

Toelichting

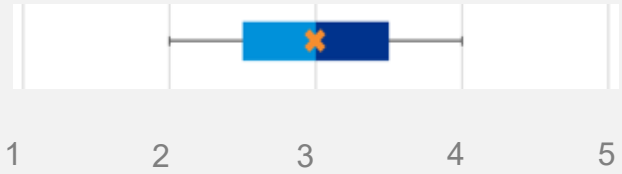
Onder ‘Risicobeleid en -proces’ worden het beleid en de bijbehorende processen verstaan die worden gebruikt met als doel het bewerkstelligen van een aantoonbare, adequate beheersing van de risico’s in relatie tot de doelstellingen van het pensioenfonds.

Resultaten

Op dit element wordt gemiddeld 3 van de 5 punten gescoord. Het integraal risicobeleid is over het algemeen integraal vastgelegd en vastgesteld, inclusief de kaders en de vereisten waaraan de uitvoering moet voldoen. Voorbeelden van ‘good practices’ binnen dit element zijn een adequate beschrijving van het datakwaliteits-beleid en de implementatie daarvan in relevante processen.

Het actueel houden van beleidsstukken en het bewaken van de consistentie tussen (vaak een grote hoeveelheid aan) beleidstukken onderling is een ontwikkelpunt voor een meerderheid van de deelnemende fondsen. Daarnaast zijn processen en bijbehorende (key) beheersmaatregelen niet altijd in kaart gebracht. Ook de aantoonbaarheid van het daadwerkelijk werken volgens de beschreven processen en het uitvoeren van beheersmaatregelen is een aandachtspunt.

Risicomonitoring en -rapportage



Uitkomsten en bijzonderheden

Op het element ‘Risicomonitoring en -rapportage’ zijn scores tussen 2 en 4 toebedeeld. De meeste scores liggen tussen 2,5 en 3,5.

Toelichting

‘Risicomonitoring en -rapportage’ betreffen de activiteiten om risico’s te identificeren, te beoordelen, te prioriteren en erover te rapporteren. Het doel hiervan is inzicht te krijgen in de mate waarin relevante risico’s impact hebben op het behalen van de doelen van het pensioenfonds. Daarnaast geven deze inzicht in de wijze waarop wordt omgegaan met de geïdentificeerde risico’s, door deze te vermijden, te accepteren, te delen of beheersmaatregelen te implementeren met als doel de risico’s te beheersen en te mitigeren.

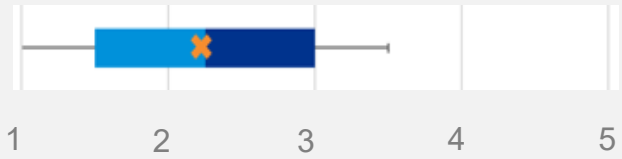
Resultaten

Op dit element wordt gemiddeld 3 van de 5 punten gescoord. De risicomanagement-cyclus wordt doorlopen en het proces voor identificatie, meting en beheersing van risico’s is geformaliseerd en vastgelegd. Risico’s worden integraal beoordeeld, waarbij ook aandacht is voor de samenhang tussen risico’s en de gerapporteerde KRI’s. Hierbij merken we op dat bij veel fondsen een verschil in de mate van volwassenheid tussen de financiële en niet-financiële risico’s wordt onderkend. De monitoring en rapportage omtrent de niet-financiële risico’s zijn bij een meerderheid van de fondsen nog onvoldoende. Dat hangt samen met de bevinding dat de risicobereidheid voor niet-financiële risico’s verder kan worden uitgewerkt.

Bij veel deelnemende fondsen is de eerste lijn nog beperkt betrokken bij het opstellen van rapportages over risico’s en risicobeheersing. Daarnaast verdient de opvolging van aandachtspunten en aanbevelingen in risicomanagementrapportages soms meer aandacht.

Voor fondsen die cruciale processen hebben uitbesteed geldt als aanvullend aandachtspunt het samenbrengen / afstemmen van de eigen rapportage(s) op/met die van de uitbestedingspartij(en), zodat het bestuur op efficiënte wijze over de benodigde stuurinformatie over alle relevante (key) risico’s beschikt.

Data en systemen



Uitkomsten en bijzonderheden

Op het element ‘Data en systemen’ zijn scores tussen 1,5 en 3,5 toebedeeld en dit is hiermee het laagst scorende element uit dit onderzoek. De meeste scores liggen tussen 1,5 en 3.

Toelichting

Binnen het element ‘Data en systemen’ is de mate van gebruik van geïntegreerde, fondsbrede systemen voor risicobeheersing (GRC-tooling) beoordeeld.

Resultaten

Op dit element wordt gemiddeld 2,1 van de 5 punten gescoord, waarmee dit de laagste score in dit onderzoek is. Er is op onderdelen een infrastructuur voor risicomanagement aanwezig en er wordt in beperkte mate gebruikgemaakt van eigen informeel ontwikkelde en gestandaardiseerde tools. Indien van toepassing wordt zo mogelijk gesteund op de tooling zoals aanwezig bij de uitvoerder, maar dit is niet altijd het geval.

Er kan nog een stap worden gezet om risicomanagement de middelen en infrastructuur te geven om taken effectief en efficiënt uit te kunnen voeren. Daarnaast kan tooling een grotere bijdrage leveren aan de mate van aantoonbaarheid van het risicomanagement.

KPMG

Conclusies

Conclusie

Uit het onderzoek is gebleken dat de gemiddelde score op alle elementen van het risicomanagementraamwerk rond 3 ligt, met uitzondering van de score op het element ‘Data en systemen’. Of deze score ook als een voldoende gezien mag worden, is mede afhankelijk van de situatie en ambitie van het pensioenfonds zelf. De vereisten ten aanzien van een integere en beheerste bedrijfsvoering vullen dit niet voor het pensioenfonds in (zie ook bijlage II).

In het algemeen zijn wij van mening dat gestreefd zou moeten worden naar een niveau waarop het risicomanagement aantoonbaar, integraal en effectief wordt uitgevoerd, waarbij de kosten opwegen tegen de baten. De vertaling hiervan naar een ambitieniveau verschilt per element en is onder meer afhankelijk van de omvang van het pensioenfonds, de aard en complexiteit van de risico’s die gelopen worden en de mate waarin zaken zijn uitbesteed. In het algemeen zal dit tot een gewenste score van ten minste 3 en op onderdelen 4 leiden.

Deelnemers aan de benchmark scoren in het algemeen goed ten aanzien van de beheersing van de financiële risico’s. In het algemeen zien wij dat ten aanzien van de beheersing van de niet-financiële risico’s meer diepgang kan worden bereikt.

Op basis van ons onderzoek zien we de volgende **drie** aandachtspunten voor de korte termijn:

Aantoonbaarheid

Het aantoonbaar in control zijn kost veel pensioenfondsen nog moeite. De uitvoering van beheersmaatregelen wordt vaak niet centraal gemonitord, waardoor inzicht in welke risico’s niet adequaat worden beheerst ontbreekt. De benodigde rapportages voor interne en externe belanghebbenden resulteren nog vaak in een verscheidenheid aan deels overlappende documenten die ad hoc worden opgesteld.

Governance

De scheiding tussen de lijnen binnen het ‘three lines model’, evenals de borging van de onafhankelijkheid van elke lijn, kan nog worden verbeterd. Rolverdeling en invulling hiervan zijn veelal op papier wel vastgelegd, maar de werking in de praktijk kan worden verbeterd. Kennis van specifieke risico’s, zoals IT-risico’s, is niet altijd in voldoende mate aanwezig, en afhankelijk van individuen. Dit geldt voor zowel de eerste als de tweede lijn.

Grip op uitbesteding

Enerzijds zélf in control blijven over de eigen uitbestedingsrisico’s en anderzijds niet op de stoel van de uitbestedingspartij gaan zitten is een lastige balans. Momenteel wordt vaak nog (te) veel gesteund op de analyses en rapportages van de uitbestedingspartij, zonder dat daarbij de link naar de risico’s en risicobereidheid van het fonds zelf wordt gelegd.

Uit deze benchmark blijkt dat de sector in het algemeen nog een stap kan zetten ten aanzien van het gebruik van (GRC-)tooling. Tooling kan daarnaast ook een rol spelen bij het adresseren van bovenstaande aandachtspunten.

Contactgegevens

Veronique de Boer-Achmad
Financial Risk Management
Senior Manager
Tel: 06 10 77 52 67
deboer-achmad.veronique@kpmg.nl

Bianca Meijer
Financial Risk Management
Senior Manager
Tel: 06 53 29 79 15
meijer.bianca@kpmg.nl

KPMG

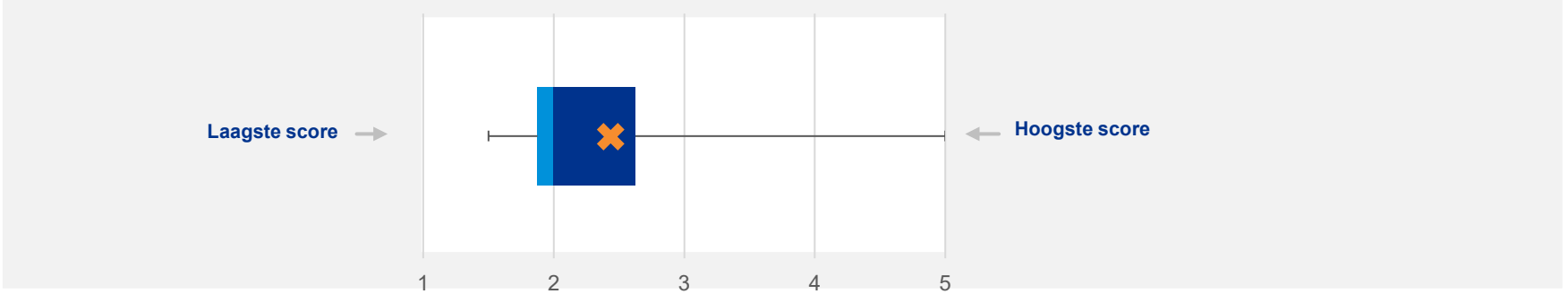
Bijlagen

I Leeswijzer boxplot
II Relevante wet- en regelgeving
III Beoordelingskader volwassenheidsniveau

Bijlage I - Leeswijzer boxplot

Een boxplot is een vereenvoudigde grafische weergave van de verdeling van data. Aan de hand van een voorbeeld wordt uitgelegd hoe u deze weergave kunt lezen. In dit voorbeeld zien de scores er, gesorteerd op hoogte, als volgt uit:

Pensioenfonds	1	2	3	4	5	6	7	8	9	10	11	12
Score	1.5	1.5	1.5	2	2	2	2	2.5	2.5	3	3.5	5
Kwartiel	1	1	1	2	2	2	3	3	3	4	4	4



1. Minimum: de laagst toebedeelde score (1,5), zie de staart aan de linkerkant
2. Tweede kwartiel *Q2:* 25 - 50% van de scores, zie het lichtblauwe blok
3. Mediaan: het middelste getal in de scorereeks (2), de kleurensplit tussen
4. Derde kwartiel *Q3:* 50 - 75% van de scores, zie het donkerblauwe blok
5. Maximum: de hoogst toebedeelde score (5), zie de staart aan de rechterkant
6. Gemiddelde van alle scores (2,4), zie het oranje kruis

In dit rapport zien we een ‘bijzondere’ boxplot bij de elementen ‘Risicostrategie en -bereidheid’ en ‘Governance en organisatie’:

- Het derde kwartiel valt over het tweede kwartiel . Dat betekent dat er een lage mate is van spreiding; de hoogste waarde in het tweede kwartiel is gelijk aan de laagste waarde in het derde kwartiel.

Bijlage II – Relevante wet- en regelgeving

De eisen ten aanzien van het risicobeheer binnen de pensioensector betreffen met name open normen waaraan door fondsen zelf invulling moet worden gegeven

In de Nederlandse wet is integraal risicomanagement in het bijzonder verankerd in de artikelen 33 en 42 van de Wet verplichte beroepspensioenregeling ter waarborging van goed bestuur en artikel 143 Pensioenwet en artikel 138 van de Wet verplichte beroepspensioenregeling ter waarborging van een beheerste en integere bedrijfsvoering.

Nadere regels met betrekking tot beheerste en integere bedrijfsvoering zijn opgenomen in artikel 18 tot en met 22 Besluit FTK. Deze hebben betrekking op het beheersen van bedrijfsprocessen en bedrijfsrisico's, integriteit en soliditeit van het pensioenfonds en de verplichting om een continuïteitsanalyse uit te voeren.

Beheersing ziet ook op eventuele uitbesteding (artikel 34 Pensioenwet dan wel artikel 43 van de Wet verplichte beroepspensioenregeling). Nadere regels met betrekking tot uitbesteding zijn opgenomen in artikel 12 tot en met 14 Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling (Besluit uitvoering Pw en Wvb).

IORP II bevat daarnaast een breed scala aan vereisten. Deze gelden grotendeels als aanvulling op de reeds bestaande wet- en regelgeving. De drie belangrijkste onderdelen zien toe op (1) verplichte sleutelfuncties, (2) een jaarlijkse ERB en (3) inzicht in ESG-factoren.

De wettelijke vereisten ten aanzien van de invulling van het risicomanagement betreffen met name open normen waaraan door fondsen zelf nader invulling moet worden gegeven. Daarbij zien we dat de verwachtingen van de toezichthouder steeds verder toenemen.

Bijlage III – Beoordelingskader volwassenheidsniveau (1/2)

	1. Initieel	2. Reproduceerbaar en informeel	3. Gedefinieerd	4. Beheerst en meetbaar	5. Continu verbeteren
1. Risicostrategie en -bereidheid 	Er is geen vastgelegde risicostrategie en -bereidheid. Doelstellingen voor risicomanagement zijn niet geformuleerd en risicomanagement maakt geen deel uit van de strategie.	De risicostrategie en -bereidheid zijn op hoofdlijnen gedocumenteerd, maar niet vastgesteld. Doelstellingen voor risicomanagement zijn informeel en worden impliciet meegenomen in de strategie van de organisatie.	De risicostrategie en -bereidheid zijn integraal gedocumenteerd en vastgesteld. Er zijn doelen voor risicomanagement geformuleerd en deze maken deel uit van de strategie van de organisatie.	De risicostrategie en -bereidheid worden periodiek geëvalueerd en aan uitkomsten van evaluaties wordt opvolging gegeven. Doelstellingen ten aanzien van risicomanagement worden geëvalueerd en maken deel uit van de evaluatie van de (bedrijfs)prestaties.	Er wordt continu gezocht naar mogelijkheden om de risicostrategie te verbeteren en doelstellingen aan te scherpen door middel van self-assessments en actief gebruik van externe bronnen.
2. Governance en organisatie 	Het ‘three lines of defence’-model is ten dele opgezet, waarbij rollen en verantwoordelijkheden niet of beperkt zijn vastgelegd. Risicomanagement vormt geen standaardonderdeel van de besluitvorming.	De functies van het ‘three lines of responsibilities’-model zijn ingericht, maar rollen en verantwoordelijkheden zijn in beperkte mate gedocumenteerd en niet integraal vastgesteld. Risicomanagement maakt niet standaard deel uit van de besluitvorming. De benodigde kennis en competenties voor een goed risicomanagement zijn bekend, maar niet vastgesteld.	Het ‘three lines of responsibilities’-model is formeel vastgesteld en geïmplementeerd met een duidelijke toewijzing van rollen en verantwoordelijkheden. Risicomanagement maakt standaard deel uit van de besluitvorming. Er is een duidelijk beeld van de benodigde kennis en competenties voor een gedegen risicomanagement en er is beleid om deze op peil te houden.	Het ‘three lines of responsibilities’-model wordt in de praktijk doorleefd, waarbij gehandeld wordt in lijn met de rollen en verantwoordelijkheden. De werking van het ‘three lines of defence’-model en de wijze waarop invulling is gegeven aan het beleid ten aanzien van kennis en competenties worden periodiek geëvalueerd en naar aanleiding hiervan worden verbeteringen doorgevoerd.	Als onderdeel van de bedrijfsvoering wordt doorlopend gezocht naar mogelijkheden om de werking van het ‘three lines of responsibilities’-model te verbeteren. Hierbij wordt gebruikgemaakt van externe bronnen.
3. Risicobeleid en -proces 	Risicobeleid en -processen zijn in beperkte mate vastgelegd. Er ontbreken duidelijke kaders en vereisten voor de uitvoering van taken.	Risicobeleid en -processen zijn op hoofdlijnen gedocumenteerd, maar zijn niet integraal vastgesteld. Er wordt uitvoering aan taken gegeven op een gestructureerde manier, maar de kaders waarbinnen dit gebeurt en de vereisten zijn informeel.	Risicobeleid en -processen zijn integraal vastgelegd en vastgesteld inclusief de kaders waarbinnen en de vereisten waaraan de uitvoering moet voldoen.	Het risicobeleid en de -procedures worden periodiek geëvalueerd zowel qua opzet en inhoud als qua uitvoering. Aan de evaluatie wordt concreet follow-up gegeven. De kwaliteit van de sturingsinformatie wordt periodiek geëvalueerd.	Het risicobeleid en de -procedures worden doorlopend geëvalueerd en er wordt gezocht naar verbeteringen. Hierbij wordt actief gebruikgemaakt van externe bronnen.

Bijlage III – Beoordelingskader volwassenheidsniveau (2/2)

	1. Initieel	2. Reproduceerbaar en informeel	3. Gedefinieerd	4. Beheerst en meetbaar	5. Continu verbeteren
4. Risicomonitoring en -rapportage 	De risicomanagementcyclus wordt in beperkte mate doorlopen. Risico's worden niet actief geïdentificeerd en gemeten en deze worden ad hoc beoordeeld. Er wordt niet gebruikgemaakt van scenarioanalyses en de effectiviteit van beheers-maatregelen wordt niet gemonitord en geëvalueerd. Rapportages zijn summier.	De risicomanagementcyclus wordt doorlopen, maar dit is niet vastgelegd. Risico's worden actief geïdentificeerd, gemeten en beoordeeld, maar niet integraal en in samenhang. Formele vastlegging ontbreekt veelal. De effectiviteit van risicomanagement wordt niet standaard beoordeeld en geëvalueerd. Er zijn risicorapportages, maar de vereisten hiervoor zijn niet vastgesteld en lenen zich beperkt voor sturing.	De risicomanagementcyclus wordt doorlopen en het proces voor identificatie, meting en beheersing van risico's is geformaliseerd en vastgelegd. Risico's worden integraal beoordeeld inclusief de samenhang. Risico's worden in samenhang met elkaar gemeten met gebruikelijke technieken. Periodiek worden scenarioanalyses uitgevoerd. Rapportages bevatten de vereisten van de gebruikers en vormen een effectief sturingsmiddel.	De risicomanagementcyclus wordt periodiek doorlopen, met een zichtbare rol voor de stap evaluatie in de cyclus. Cycli zijn niet op zichzelf staand, maar volgen elkaar op, met aandacht voor de uitkomsten. Hierbij wordt gebruikgemaakt van state-of-the-art technieken voor scenarioanalyses. De evaluaties leiden tot een concreet actieplan dat vervolgens wordt omgezet. Er wordt gestuurd op risicorapportages en de kwaliteit van de sturingsinformatie wordt periodiek geëvalueerd.	De risicomanagementcyclus wordt continu doorlopen waarbij gezocht wordt naar nieuwe risico's en vergroting van de kwaliteit van de beoordeling en meet-methoden, gebruikmakend van de state-of-the-art technieken. Hierbij wordt actief gebruikgemaakt van externe bronnen. Risicomanagement en de kwaliteit van risicorappor-tages worden doorlopend geëvalueerd en er wordt gezocht om deze te verbeteren.
5. Data en systemen 	De infrastructuur en middelen voor risicomanagement zijn beperkt. Er zijn in beperkte mate tools beschikbaar, maar deze zijn afhankelijk van individuen.	Er is op onderdelen een infrastructuur voor risico-management en er zijn middelen aan toegewezen. Er wordt in beperkte mate gebruikgemaakt van eigen informeel ontwikkelde gestandaardiseerde tools.	Risicomanagement beschikt over de middelen en infrastructuur om zijn taken effectief en efficiënt uit te voeren. Hierbij wordt op onderdelen gebruikgemaakt van tooling die in de markt aanwezig is en er zijn deels geautomatiseerde dashboards.	Risicomanagement heeft de middelen en tooling om een integraal risicomanagement effectief en efficiënt uit te voeren. Dashboards zijn geautomatiseerd. De middelen en tooling worden periodiek geëvalueerd en verbeteringen naar aanleiding hiervan worden uitgevoerd.	Risicomanagement beschikt over geavanceerde tooling en over ruime middelen om een state-of-the-art risicomanagement op te zetten en doorlopend uit te voeren.

Note: Het element 'Cultuur en gedrag' is niet beoordeeld in deze benchmark. Om die reden is dit element ook niet opgenomen in het beoordelingskader.

KPMG

KPMG on social media

KPMG app