BEDRIJFSPENSIOENFONDS
MOLENAARS
Stichting Molenaarspensioenfonds

16-9-2019

Stichting Molenaarspensioenfonds
Integraal risicomanagementbeleid 2019

Documentbeheer

Wijzigingshistorie

Versie	Datum	Naam/auteur	Wijziging
0.1	**12 mei 2019**	S&V	Eerste concept op basis van aangepaste governance (o.b.v. IORP II) en stappen gezet in volwassenheid
0.2	**15 juli 2019**	**S&V**	Aanpassingen na bespreking in IRM-commissie 11 juli.
0.3	**5 september 2019**	**S&V**	Aanpassingen ten behoeve van bestuursvergadering 16 september.

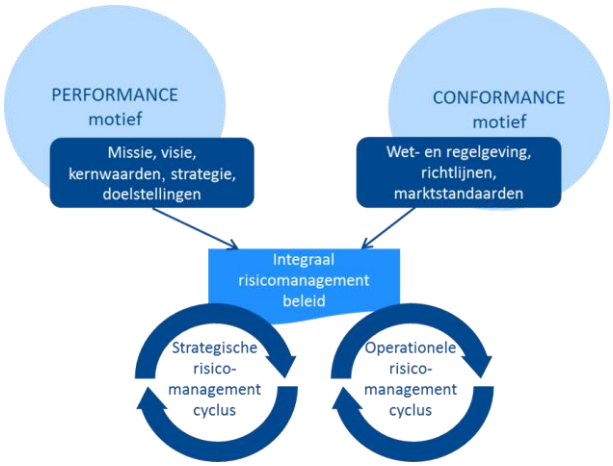
Onderdelen risicomanagement	Status	Update
RACI	In concept gereed	ntb
Risicohouding bestuur	Vastgesteld	ntb
Risicobereidheidprincipes	Vastgesteld	ntb
Risicotolerantiegrenzen	Vastgesteld	ntb
Strategische risico's	Vastgesteld	ntb
Operationele risico's	Vastgesteld	ntb

Inhoudsopgave

1. Inleiding

1.1. Doel

De Stichting Molenaarspensioenfonds (hierna het fonds) heeft het beleid met betrekking tot integraal risicomanagement (hierna: IRM) vastgelegd. Het doel van IRM is om bij te dragen aan de realisatie van de missie, visie, kernwaarden en de strategische doelstellingen van het fonds, rekening houdend met relevante wet- en regelgeving en marktstandaarden, respectievelijk het performance- en conformance motief.



Dit document geeft weer hoe het fonds het beleid op het gebied van IRM heeft vormgegeven. Het IRM-beleid is het beleidskader voor de toepassing en toetsing van de beleidsvorming en –uitvoering. Dit gebeurt op strategisch, operationeel en thematisch niveau, in samenhang, en wel als volgt:

<u>Strategisch niveau (strategische risicomanagementcyclus)</u>

- Het bestuur signaleert en onderkent tijdig interne en externe ontwikkelingen.
- Het bestuur communiceert over het strategisch normenkader, die als resultaat voortkomt uit de strategische risicomanagementcyclus (risicohouding, risicobereidheid, risicotolerantie, strategische risico's, strategische beheersing).[1]
- Het monitoren van de strategische risico's en beheersing daarvan voor de gehele procesketen om vast te stellen dat het (netto) risico binnen de risicohouding en risicobereidheid blijft.
- Het strategisch normenkader vormt de basis voor de uitvoerders om hun werkzaamheden hierop af te stemmen en hierover te rapporteren.
- Voorstellen voor beleidsaanpassing worden getoetst aan de kaders van het risicoraamwerk. Uit de risicoparagraaf (vanuit de 1e lijn) en de risico opinie (vanuit de 2e lijn) in de voorlegger blijkt de impact van het beleidsvoorstel op bestaande (strategische en operationele) risico's. De genomen besluiten worden inclusief (risico)onderbouwing vastgelegd in notulen.
- De implementatie van nieuwe/gewijzigde wet- en regelgeving start met een impactanalyse op het IRM-beleid: het risicoraamwerk, en mogelijke gevolgen voor het risicomanagementproces en de governancestructuur. De inhoudelijke beleidsherijking start nadat de kaders zijn afgebakend op basis van impactanalyse vanuit het risicoraamwerk.
- De elementen in de strategische risicomanagementcyclus (risicohouding, risicobereidheid, risicotolerantie, scenario's, strategische risico's, strategische beheersing, externe transparantie) worden tenminste eenmaal per jaar - en

[1] De risicohouding, risicobereidheid en risicotoleranties vormen als geheel het strategisch normenkader van het fonds.

zoveel eerder bij een bepaalde risicotrigger (als opgenomen in ERB-beleid) - en bij evaluatie van de strategie, door het bestuur herijkt en vastgelegd in dit risicobeleidsdocument Het IRM-beleid is onderdeel van de Actuariële en bedrijfstechnische nota.
- Het bestuur legt verantwoording af over de werking van het risicoraamwerk aan haar stakeholders onder andere via de risicomanagement paragraaf bestuursverslag conform de Richtlijnen voor de Jaarrekening (RJ-400).
- Van nieuwe (aspirant) bestuurders wordt de risicohouding vastgelegd. Op basis daarvan wordt een analyse gemaakt van de mogelijke impact van deze risicohouding op de 'boardroom dynamics' in bestuur en commissies.

<u>Samenhang strategisch- en operationeel niveau</u>
- Het bestuur realiseert bij het strategisch normenkader passende afspraken voor de uitvoering in de gehele procesketen. Afspraken zijn vastgelegd in beleid, reglementen en mandaten van commissies, contracten, SLA's, rapportage-indicatoren: KPI's en KRI's en procedures.
- Het bestuur realiseert informatievoorziening vanuit de gehele procesketen van zodanig niveau dat het bestuur kan toetsen op conformiteit van de uitvoering met het strategisch normenkader en waar nodig kan bijsturen.

<u>Operationeel niveau (operationele risicomanagementcyclus)</u>
- Het monitoren van de operationele risico's en beheersing daarvan voor de gehele procesketen om vast te stellen dat het (netto) risico binnen de risicohouding en risicobereidheid blijft.
- De elementen in de operationele risicomanagementcyclus (operationele risico's en beheersing, informatievoorziening en verantwoording vanuit uitvoerders) worden tenminste eenmaal per jaar en bij materiële veranderingen, door het bestuur herijkt.

<u>Thematisch niveau</u>
- Het periodiek uitvoeren van risicoanalyses door de gehele procesketen van het fonds op specifieke thema's zoals IT, Privacy en integriteit (SIRA).

1.2. Positionering en reikwijdte van het beleid

Het IRM-beleid is een nadere uitwerking van de kaders in de ABTN. Het IRM-beleid stelt op haar beurt de (risicomanagement-)kaders voor overige beleidsterreinen, waaronder uitbestedingsbeleid, informatiebeveiligingsbeleid, integriteitsbeleid en beleggingsrisico-beleid.

Het beleid heeft betrekking op alle type risico's en op de gehele strategische en operationele bedrijfsvoering van het fonds. Indien delen van de bedrijfsvoering zijn uitbesteed aan derden, dan waarborgt het bestuur, en ziet daar op toe, dat deze derden het beleid naleven.

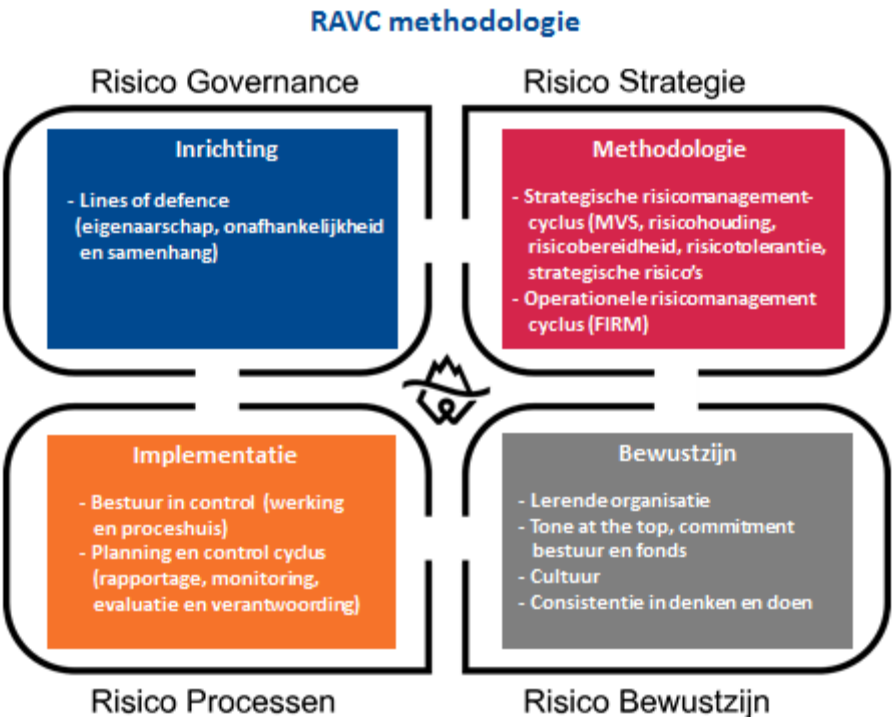
Van het beleid kan alleen na overleg met de voorzitter van de IRM-commissie en met goedkeuring van het bestuur worden afgeweken. Deze afwijking wordt beargumenteerd en schriftelijk vastgelegd.

1.3. Stappenplan (methodologie) voor integraal risicomanagement

Om IRM te implementeren in beleidsprocessen, wordt er een indeling gekozen om de strategie van het fonds te versterken. Dit gebeurt door het werk- en denkmodel van het Risk Appetite Value Chain RAVC-kwadranten model. Dit model geeft de inrichtings-elementen van het integraal risicoraamwerk weer. Binnen het integraal risico-management raamwerk maken we onderscheid naar de vier kwadranten zowel in de strategische- alsook in de operationele cyclus (zie afbeelding hieronder – en voor een nadere toelichting bijlage B1.1).

Het gaat in beide cycli namelijk om het volgende:

Inrichtingsvraagstuk:	Welke inrichting kiezen wij, welke inrichting past bij ons fonds (Risico Governance);
Methodologisch vraagstuk:	Langs welk plan van aanpak werken wij, volgens welke strategie en methodologie (Risico strategie);
Proces vraagstuk:	Wat gaan we doen, en waar in ons proceshuis past dat (Risico Processen);
Bewustzijnsvraagstuk:	Weten we wat er moet gebeuren en waarom het van belang is, en wat is onze risicocultuur (Risico Bewustzijn).



1.4 Beheer en vaststelling van het beleid

Het IRM-beleid wordt beheerd door de Integraal Risicomanagement commissie (hierna de IRM-commissie). Het bestuur van het fonds stelt het beleid vast. Het bestuur is eindverantwoordelijk voor de naleving van het beleid. Namens het bestuur ziet de IRM-commissie hierop toe. Het fonds evalueert jaarlijks de opzet van het beleid en past het beleid indien gewenst aan.

Jaarlijks stelt de IRM-commissie een IRM-jaarplan op ten behoeve van alle commissies en het bestuur, op basis waarvan invulling wordt gegeven aan het beleid. Het IRM-jaarplan wordt goedgekeurd door het bestuur. De commissies in de eerste lijn en de IRM-commissie zetten hun eigen jaarplan op in Q4 voor het daarop volgende jaar. De IRM-commissie bekijkt de jaarplannen van de andere commissies vanuit haar challengende rol. De jaarplannen kunnen worden aangepast op basis van vaststellingen door de IRM-commissie.

1.5 Leeswijzer

Dit beleidsdocument is opgezet in lijn met het RAVC-vier kwadrantenmodel (hierna: stappenplan) en wel als volgt. Hoofdstuk 2 beschrijft de fonds specifieke Risico governance. Hoofdstuk 3 (Risico strategie) en hoofdstuk 4 (Risico processen) beschrijven de fonds specifieke invulling aan de hand van de 8 stappen van het risicoraamwerk. Hoofdstuk 5 beschrijft het risicobewustzijn. In hoofdstuk 6 is de datum weergegeven waarop dit beleid door het bestuur voor het laatst is gewijzigd en vastgesteld.

In bijlage 1 worden de gehanteerde modellen inhoudelijk toegelicht en in bijlage 2 zijn definities opgenomen.

2. Risico Governance

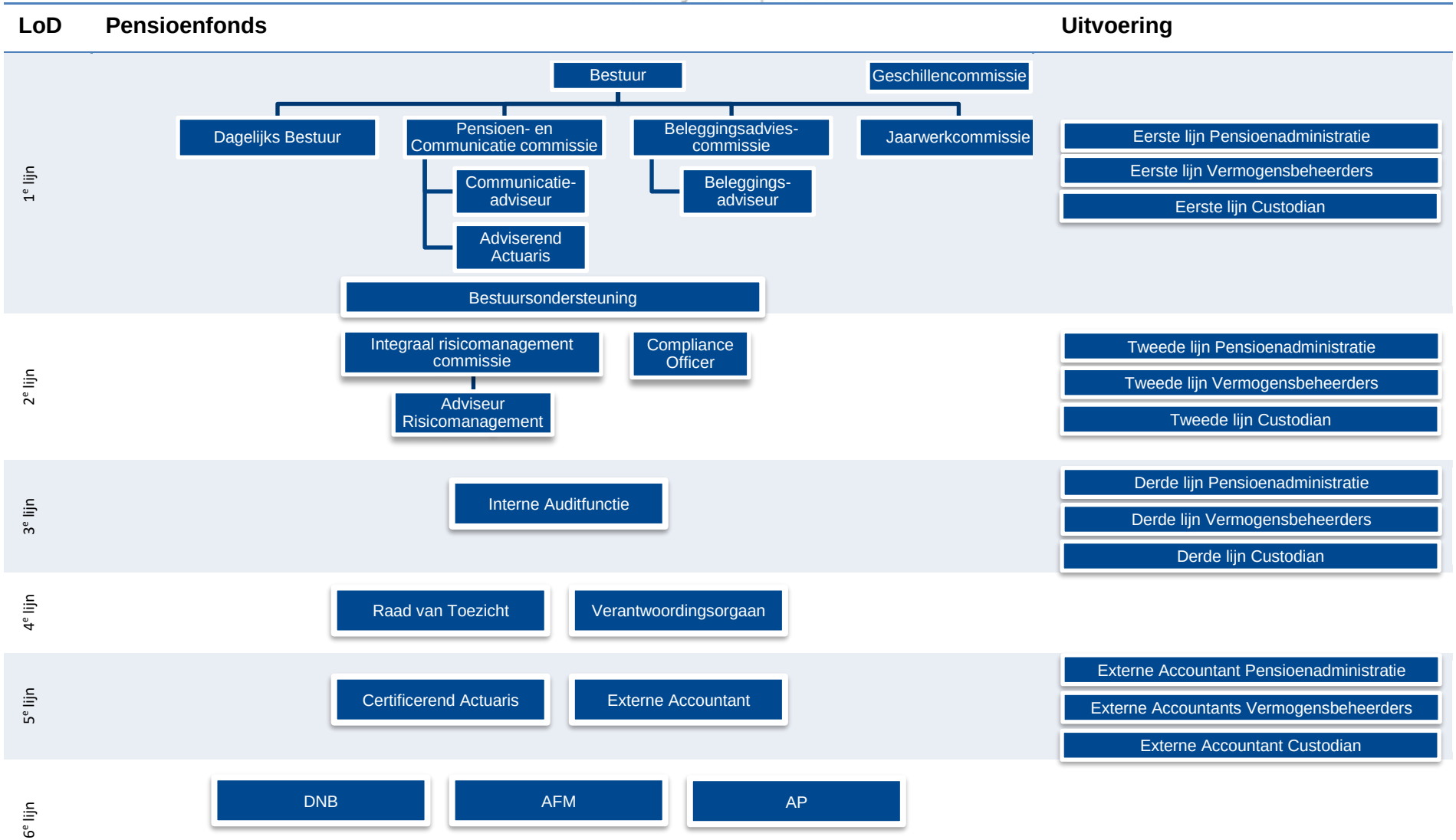
2.1. Doel

Dit hoofdstuk beschrijft de verankering van het risicoraamwerk binnen de governancestructuur van het fonds en heeft tot doel de taken, verantwoordelijkheden en bevoegdheden van de functies binnen de governance te beschrijven. Hoe de rollen zich tot elkaar verhouden wordt toegelicht met het principe van de 'six lines of defence'. In paragraaf 2.3 is de governancestructuur schematisch weergegeven. Het doel hierbij is dat de gekozen governance van ons fonds, onze strategie dient te versterken. Daar waar dit niet het geval is, zal er een evaluatie plaatsvinden.

2.2.Organisatiestructuur en lines of defence

In onderstaande figuur is het organogram van het pensioenfonds weergegeven. De rollen van de verschillende actoren zijn beschreven in de ABTN en in de verschillende reglementen.

BEDRIJFSPENSIOENFONDS
MOLENAARS
Stichting Molenaarspensioenfonds



Het pensioenfonds hanteert het concept 'six lines of defence (verdedigingslinies)' zoals getoond in onderstaande tabel. Dit is het basisprincipe waarop de rolverdeling tussen actoren met een doorkijk door de hele keten van 'assurance'. Alle lijnen dienen elkaar te versterken.

Line of defence		Toelichting
1e lijn	Bestuur en commissies	*(Eind)Verantwoordelijk* voor de uitvoering van het primaire proces inclusief risicobeheersing. Het vertrekpunt hierbij is dat het bestuur besluiten neemt en de commissies besluit voorbereidend zijn. De goedgekeurde jaarplannen van de commissies en de taakomschrijvingen en mandaatregelingen gelden als mandaat. *Beleidsvorming* • Kaderstellend aan het bestuurlijke proces • Richtinggevend voor uitvoering primaire proces. • Implementeren van governance en risicoraamwerk. • Monitoring en evaluatie van de algehele governance • Integraal management, inclusief risicomanagement *Uitvoering* • Het zorgdragen voor de beheerste en integere uitvoering van het primaire proces. • Het beheersen van risico's. • Het monitoren, rapporteren en bijsturen. • Het zorgdragen voor risicobewustzijn. • Verantwoording afleggen aan de Raad van Toezicht. *Periodiciteit* Jaarlijks wordt een commissievergadering expliciet ingericht voor de risicomanagementactiviteiten. Daarnaast zijn risicomanagementactiviteiten al geïntegreerd in de besluitvormingsprocessen en rapportagecycli. *Resultaat* • Jaarplan. • Risicoparagraaf in voorleggers. • Actueel en passend beleid. • (Risico)rapportage bestuursbureau. • Beoordeling uitvoerders (SLA: KPI & KRI, ISAE, Incidenten, SIRA, IT en BCM). • Zelfevaluatie bestuur. • Uitbestedingsbeleid. • Integriteitsbeleid.
2e lijn	Risk en Compliance	*Management Services* rol naar bestuur en commissies: *Challengen* van voorgenomen besluiten. Het vertrekpunt hierbij is dat de commissies, adviserend en voorbereidend zijn naar het bestuur. Risicomanagement (sleutelfunctie IORP II) en compliance zijn onderdeel van de 2e lijn. *Beleid* • Inrichting van governance en risicoraamwerk en beheer van het risicomanagement beleid

		• Monitoring of bij uitvoering van processen raamwerk wordt gevolgd. • Zorgdragen voor rapportages hierover. *Uitvoering* • Het beoordelen, monitoren en rapporteren van financiële en niet-financiële risico's in de strategische- en operationele risicomanagementcyclus aan het bestuur. • Het vervullen van een initiërende en adviserende rol bij de vormgeving van het risicobeheer. • Het bijdragen aan de beheersing van het risicoprofiel • Toetsen van de risicobeoordeling bij voorgenomen beleidsbesluiten. • Het leveren van input vanuit het onafhankelijke risicomanagementperspectief door middel van overwegingen en adviezen in voorleggers (countervailing power) • Ondersteuning bij monitoring of bij uitvoering van processen raamwerk wordt gevolgd. • Het faciliteren van de reguliere risico-identificatie (strategische risico's, FIRM, FOCUS, RAVC) • Het verzorgen van de monitoring en rapportages van de risico's en het risicoprofiel van het fonds. • Gevraagd en ongevraagd adviseren. *Periodiciteit* Is aangegeven in RACI tabel. *Resultaat* • Jaarplan. • Risico opinie bij voorleggers. • IRM dashboard. • Actueel en passend IRM-beleid. • Zelfevaluatie IRM. • Risicoparagraaf in jaarverslag
3e lijn	Interne Auditfunctie	*Management Oversight* naar eerste en tweede lijn. Het aantoonbaar toetsen van de effectiviteit van de 1e en 2e lijn in de uitvoering van het risicomanagement en compliance beleid. De in IORP II genoemde sleutelfunctie interne audit is onderdeel van de 3e lijn. *Beleid* • Review van governance en risico raamwerk. • Onafhankelijk oordeel over werking 1e en 2e lijn. *Uitvoering* • Het uitvoeren van de volgende taken: jaarlijks auditplan opstellen, 'risk-based' audits uitvoeren, afstemming met externe accountant en certificerende actuaris over administratieve organisatorische inrichting en checks & balances en prudent person. • Uitvoeren van de audits conform interne audit jaarplan • Rapporteren over de uitkomsten van de uitgevoerde audits aan het bestuur.

		Periodiciteit Op risico gebaseerde audits op basis van jaarplan. *Resultaat* • Jaarplan. • Audit rapporten.
4e lijn	Verantwoording afleggen aan de Raad van Toezicht en het verantwoordings-orgaan	*Fondstoezicht*. Beoordeelt de kwaliteit van het door het bestuur gevoerde beleid en geven daar een oordeel en aanbevelingen over op basis van statuten, code pensioenfondsen en principes van goed bestuur. De RvT houdt toezicht op het beleid van het bestuur en op de algemene gang van zaken in het fonds. Daarnaast staat de RvT het bestuur met raad ter zijde. De RvT is statutair belast met het toezien op adequate risicobeheersing en evenwichtige belangenafweging door het bestuur. Periodiek beoordeelt de RvT op strategisch niveau of de fondsactiviteiten in algemene zin passen binnen de goedgekeurde risicobereidheid. Het verantwoordingsorgaan oordeelt over het handelen van het bestuur en de uitvoering van de taken door de RvT aan de hand van het jaarverslag.
5e lijn	Externe accountant en Certificerend actuaris.	*Fondstoezicht*. Achteraf toetsen van opzet en effectiviteit van (financiële en actuariële) risicomanagement en interne beheersing. Ook op basis van de ISAE van de uitvoeringsorganisaties. De certificerend actuaris is houder en vervuller van de actuariële sleutelfunctie (IORPII). De controlerend accountant overlegt desgewenst met de externe accountant van de aangestelde pensioenadministrateur, vermogensbeheerder en custodian.
6e lijn	Externe toezicht zijnde DNB, AFM en Autoriteit Persoonsgegevens (AP).	*Sectortoezicht*. Ziet toe op uitvoering van beleid conform wet- en regelgeving (normenkaders) aan de hand van ingediende rapportages, uitgevoerde onderzoeken, sectoronderzoeken en gesprekken. DNB voert het prudentiële toezicht uit op pensioenfondsen onder andere op basis van door het pensioenfonds ingediende verplichte rapportages. AFM voert het gedragstoezicht uit en AP is de toezichthouder betreffende de correcte naleving van de Algemene Verordening Gegevensbescherming.

2.3 De (risico)governancestructuur schematisch bezien

Risicomanagement is onderdeel van het gehele raamwerk aan governance. De verantwoordelijkheidsverdeling op gebied van risicomanagement binnen MPF is vastgelegd in een RACI tabel. Dit overzicht geeft per stap in het risicomanagementproces aan wie verantwoordelijk is, wie de stap uitvoert, wie wordt geconsulteerd en wie geïnformeerd. De RACI tabel omvat naast het bestuur en bestuurscommissies ook de overige fondsorganen, de adviseurs, het bestuursbureau en de uitbestedingspartner.

De rollen en verantwoordelijkheden kunnen als volgt verdeeld zijn in het risicomanagement proces:

R = Responsible:	de partij die het werk uitvoert (verantwoordelijk voor de voorbereiding), 1 partij
A = Accountable:	opdrachtgever, verantwoordelijk dat de taak wordt uitgevoerd (besluitvorming), 1 partij
C = Consulted:	in brede zin betrokken bij de taak zonder daar zelf verantwoordelijk voor te zijn. Levert en ontvangt input, tweezijdige informatie, evt. meerdere partijen (countervailing power)
I = Informed:	wordt geïnformeerd over de taak (eenzijdige communicatie, mededeling)
Ch = Challenging:	uitdaging van eerste lijn door tweede lijn

De periodiciteit van risicomanagementprocessen is aangegeven. De aangegeven periodiciteit is een minimum en het proces zal, bijvoorbeeld in geval van een risicotrigger of anderszins vanuit risico gebaseerde aanpak, ook frequenter dan dit minimum kunnen worden uitgevoerd.

[RACI NOG OP TE NEMEN]
De RACI is in concept gereed en zal later dit jaar worden vastgesteld door het bestuur. Na vaststelling zal de RACI in dit beleidsdocument worden opgenomen.

3. Risico Strategie

Nu we het eerste kwadrant hebben doorlopen, zullen wij stilstaan bij het tweede kwadrant. Het tweede kwadrant betreft het doorlopen van de onderstaande stappen volgens de risicomanagement methodologie.

Stappenplan voor integraal risicomanagement	
Stap 1:	Missie, visie strategie en risicohouding
Stap 2:	Doelstellingen en risicobereidheid
Stap 3:	Identificeren en benoemen van risico's
Stap 4:	Wegen van risico's
Stap 5:	Beheersmaatregelen en netto risico's
Stap 6:	Borgen van beheersmaatregelen in de organisatie
Stap 7:	Informeren en communiceren
Stap 8:	Monitoren en evaluatie van het gehele proces en reflectie monitoring (bewaking)

3.1. Stap 1: Missie, visie, strategie en risicohouding

Het IRM-beleidskader start met de strategische doelstellingen, die afgeleid worden van de missie en de visie van het fonds zoals die door het bestuur zijn vastgesteld. Deze processtap behelst het door het bestuur van het fonds valideren c.q. herijken van de missie, visie, kernwaarden, strategische doelstellingen en risicohouding. Dit is onderdeel van de strategische managementcyclus van het fonds.

3.1.1 Missie, visie, kernwaarden en strategie

Het bestuur stelt minimaal eens per 3 jaar of bij grote wijzigingen haar missie, visie en strategie vast. Het bestuur toetst jaarlijks de noodzaak om de missie, visie en/of strategie bij te stellen of zoveel eerder als er sprake is van een trigger.

Onderstaand zijn de actuele missie, visie en strategische doelstellingen van het fonds weergegeven.

Missie

Het fonds heeft de volgende missie:
Het fonds wil op een verantwoorde wijze, door optimaal beheer en toezicht, de verplichtingen aan de deelnemers waarmaken.

Visie

Het fonds heeft de volgende visie:
Het fonds wil haar deelnemers nu en in de toekomst op een transparante wijze een voorspelbaar pensioen bieden.

Kernwaarden

Wij hanteren de volgende kernwaarden:
• Betrouwbaar • Transparant • Betrokken • Deskundig • Bereikbaar • Duurzaam

Strategische doelstellingen

De missie, visie en strategie van het fonds komen tot uitdrukking in de volgende doelstellingen:
1. De risico's die in de regeling aanwezig zijn, op een evenwichtig wijze afwegen over alle belanghebbenden.
2. Het betaalbaar houden van de pensioenregeling.
3. Het behalen van een passend rendement om in eerste instantie de nominale verplichtingen te kunnen nakomen en in de tweede instantie om een toeslag te kunnen verlenen.
4. Het optimaliseren van de dienstverlening aan werkgevers en deelnemers in de bedrijfstakken.
5. Een heldere communicatie over de pensioenregeling, op een transparante, persoonlijke en herkenbare wijze.

3.1.2 Risicohouding

De risicohouding van het bestuur is een reflectie van de individuele risicohouding van de bestuurders. Het vormt de basis voor de bepaling van de risicobereidheid en risicotolerantie van het fonds. Op basis van de vastgestelde risicohouding van de bestuurders wordt een analyse gemaakt van de mogelijke impact van deze risicohouding op de 'boardroom dynamics' in het bestuur en commissies.

Het fonds stelt de risicohouding van het bestuur jaarlijks vast, of bij wijziging van de missie, visie en/of strategie. Daarbij hanteert het bestuur de 5-punts-schaal conform het RAVC©-model (zie bijlage b1.4). De risicohouding kan afhankelijk zijn van de context. Het fonds hanteert, naast een algehele risicohouding voor het bestuur, vier domeinen waarvoor de risicohouding wordt vastgesteld, namelijk: besturingsfilosofie, reputatiemanagement, product & uitvoering en kapitaal management. Een korte toelichting op deze domeinen is weergegeven in bijlage b1.3. De risicohouding van het fonds is hieronder opgenomen.

Van het bestuur in zijn geheel: Kritisch (2)

De risicohouding wordt gedefinieerd als links van gebalanceerd en rechts van kritisch (op het continuum van risicozoekend naar risicomijdend, zoals weergegeven in B1.4), maar zal als kritisch worden gedefinieerd. Bij voorkeur neemt het bestuur geen risico. Indien het nemen van risico bij kan dragen aan het behalen van de doelstellingen van het fonds, is het bestuur bereid het nemen van meer risico in de besluitvorming te overwegen.

Besturingsfilosofie | *Gedrag, Leiderschap & Cultuur*
Het domein Besturingsfilosofie gaat vooral over: • Gedrag (hoe wij handelen). • Leiderschap (onze regierol in de keten met uitbestedingsrelaties). • Cultuur (bewustzijn, gericht op beheerste en integere bedrijfsvoering). • Governance (inrichting van de organisatiestructuur, rollen en verantwoordelijkheden). • De kernwaarden.
Kritisch (2)
Op cultuur, leiderschap en gedrag van het bestuur wil het bestuur weinig risico's nemen. Dit raakt aan alle doelstellingen van het fonds en moet in orde zijn.

Reputatiemanagement | *Imago, Identiteit & Integriteit*
Het domein reputatiemanagement gaat vooral over: • Het imago (hoe zien anderen ons). • De identiteit (wat wij willen uitstralen). • De integriteit (handelen volgens onze kernwaarden). • De compliance (volgens het principe 'comply or explain' voldoen aan wet- en regelgeving, waarbij onze kernwaarden leidend zijn). • De reputationele overtuigingen.
Kritisch (2)
Omdat het vertrouwen van deelnemers in het fonds cruciaal is, dient het bestuur de reputatie van het pensioenfonds zorgvuldig te bewaken. Het is belangrijk dat het fonds te allen tijde het beleid op bevredigende wijze kan uitleggen.

Product en Uitbesteding | *Producten, Regeling & (IT-)Processen*
Dit domein gaat vooral over: • De uitvoeringsprocessen. • De pensioenregeling. • De inrichting, monitoring, evaluatie en terugkoppeling ten aanzien van Service Level Agreements (SLA). • De inrichting, de monitoring, de evaluatie en de terugkoppeling ten aanzien van de (IT-)organisatie van het fonds en de uitbestedingsrelaties. • De overtuigingen ten aanzien van de producten, de markt, de klanten en de (IT-)organisatie van het fonds en de uitbestedingsrelaties.
Kritisch (2)
Op de uitvoering van de pensioenregeling, die door het fonds geheel is uitbesteed, wil het fonds weinig risico's nemen. De uitvoering dient zoveel mogelijk vlekkeloos te zijn.

Kapitaalmanagement | *Solvabiliteit, Liquiditeit & Rentabiliteit*
Het domein kapitaalmanagement gaat vooral over: • De huishouding van het fonds: dekkingsgraad, vermogensbeheer, balansmanagement, liquiditeit en kosten. • De beleggingsovertuigingen.
Gebalanceerd (3)
Beleggingsrisico lopen is noodzakelijk vanwege het streven naar koopkrachtbehoud van het pensioen.

Risicohouding nFTK in relatie tot het risicoraamwerk
Met ingang van 2015 is het pensioenfonds uit hoofde van de Pensioenwet verplicht de financiële risicohouding, volgens het nieuw Financieel Toetsingskader (nFTK) gerelateerd aan het pensioenresultaat, te concretiseren in kwantitatieve maatstaven. De in het nFTK bedoelde risicohouding vormt het kader voor:

- Het vaststellen van het beleid, bijvoorbeeld het strategisch beleggingsbleid.
- De verantwoording achteraf van het fondsbestuur over het gevoerde beleid.
- De afstemming met het verantwoordingsorgaan, de aangesloten ondernemingen en de gezamenlijke ondernemingsraad in de situatie dat het vereist eigen vermogen structureel buiten de vastgelegde bandbreedte ligt.

Deze financiële risicohouding gerelateerd aan het pensioenresultaat is gedefinieerd voor de korte en lange termijn en is vastgelegd in de ABTN.

Deze risicohouding maakt inhoudelijk onderdeel uit van het domein Kapitaalmanagement en wordt toegepast bij het definiëren van tolantiegrenzen van de risicobereidheids-principes.

Wat de wet 'risicohouding' noemt, is in de methodiek en bijbehorende definities (bijlage 2) die het fonds gebruikt 'risicobereidheid' die wordt uitgedrukt in risicobereidheids-principes en geconcretiseerd met risicotolerantie. Het betreft immers meetbare waarden, en niet een grondhouding van een individu of groep ten opzichte van risico en onzekerheid.

3.2. Stap 2: Doelstellingen en risicobereidheid

De volgende stap in de strategische managementcyclus van het fonds is het vaststellen van de strategische doelstellingen en de risicobereidheid. De strategische doelstellingen zijn een concretisering van hetgeen het fonds wil bereiken met de strategie (de performance-kant). De risicobereidheid is een concretisering van de risicohouding, door te definieëren wat het fonds niet wenst mee te maken (de risico-kant).

3.2.1 Bepalen van strategische doelstellingen

Het bestuur stelt minimaal eens per drie jaar of bij grote wijzigingen van haar missie, visie en strategie de strategische doelstellingen vast. Het bestuur toetst jaarlijks de noodzaak om de strategische doelstellingen bij te stellen, of zoveel eerder bij een risicotrigger.

Ten behoeve van het meetbaar maken van de realisatie van de doelstellingen stelt het bestuur zo concreet en meetbaar mogelijke ('key performance'-) indicatoren vast bij de strategische doelstellingen. Voor deze key performance indicatoren (KPI's en KRI's) stelt het bestuur streefwaarden vast.

3.2.2 Bepalen en valideren van de risicobereidheid

Daarnaast valideert het bestuur jaarlijks haar risicobereidheid in relatie tot de risicohouding en doelstellingen. De risicobereidheid is uitgedrukt in risicobereidheids-principes. De strategische doelstellingen en risicobereidheidsprincipes van het fonds vormen de kaders waarbinnen de strategische en operationele (risico-) managementcycli worden ingericht en uitgevoerd.

Het bestuur stelt voor elk van de domeinen vast wat het bestuur niet wenst. De uitkomst van deze analyse is leidend voor het bepalen van de risicobereidheidsprincipes. De risicobereidheidsprincipes zijn een positieve verwoording van wat het bestuur niet wenst.

Risicobereidheid het fonds
Het bestuur heeft risicobereidheidsprincipes vastgesteld. Hieronder vindt u de actuele weergave van risicobereidheidsprincipes en risicotolerantiegrenzen.

Risk appetite indicatoren en tolerantiegrenzen het fonds
Ten behoeve van het meetbaar maken van de bandbreedtes voor de risicobereidheid worden de risicobereidheidsprincipes verder geconcretiseerd door risicotolerantie. De **risicotolerantie** is uitgedrukt in **criteria (risk appetite indicators)** met grenzen uitgedrukt in een streefwaarde, 'ondermaats' en 'bovenmaats'. Risicotolerantie – als toetssteen voor de (in volgende processtappen te bepalen) risico's en het risicobeheer – de verbinding tussen risicomanagement en performancemanagement. De toepassing van risicotolerantie wordt gerealiseerd door bandbreedtes te verankeren in beleid, afspraken met dienstverleners en de (risico-)management rapportages. Samen met de KPI's vormen zij de verbinding tussen risicomanagement en performancemanagement.

De risicotolerantiegrenzen zijn uitgedrukt in een minimum-, streef- en maximumwaarde. De streefwaarde duidt op een waarde die het bestuur, gezien de gekozen risicohouding, nastreeft. De ondergrens (ondermaats) geeft aan welke waarde het bestuur, gezien de risicohouding ongewenst acht, en waarop dient te worden bijgestuurd. De maximumwaarde (bovenmaats) kan een indicatie zijn van het feit dat er te weinig risico wordt gelopen en/of te veel geïnvesteerd wordt in het beheersen van het risico.

BEDRIJFSPENSIOENFONDS
MOLENAARS
Stichting Molenaarspensioenfonds

Risicobereidheid en –tolerantie Besturingsfilosofie (Risicohouding: kritisch)

	Risicobereidheidsprincipes		Risk Appetite indicator	streefwaarde	ondermaats <	bovenmaats >
1	Wij willen bestuursleden die integer zijn als mens en bestuurslid	1	Aantal compliance issues aangemerkt door externe compliance officer	0	1	-1
2	Wij willen voorkomen dat cao conflicten onderdeel zijn van de bestuurstafel.	2	Aantal keren in afgelopen 12 maanden dat de zelfevaluatie en persoonlijke reflectie besproken zijn tijdens zelfevaluatie	1	0	2
3	Wij willen dat bestuursleden 'veilig' en zonder last en ruggenspraak kunnen spreken	3	Aantal keren in afgelopen 12 maanden dat de zelfevaluatie en persoonlijke reflectie besproken zijn tijdens zelfevaluatie	1	0	2
4	Wij staan open voor kritiek en argumenten	4	Aantal keren in afgelopen 12 maanden dat de zelfevaluatie en persoonlijke reflectie besproken zijn tijdens zelfevaluatie	1	0	2
5	Wij handelen uitsluitend in het belang van het fonds en haar stakeholders	5	Aantal keren in afgelopen 12 maanden dat de zelfevaluatie en persoonlijke reflectie besproken zijn tijdens zelfevaluatie	1	0	2
6	Bij alle vraagstukken wegen wij de risico's en nemen die mee in de besluitvorming.	6	Aantal bestuursbesluiten zonder voorlegger	0	1	-1
7	Wij willen dat andere fondsorganen in hun eigen rol blijven	7	Aantal keren in afgelopen 12 maanden dat de zelfevaluatie en persoonlijke reflectie besproken zijn tijdens zelfevaluatie	1	0	2
8	Wij willen een evenwichtige inbreng van bestuursleden en dat men naar elkaar luistert	8	Aantal keren in afgelopen 12 maanden dat de zelfevaluatie en persoonlijke reflectie besproken zijn tijdens zelfevaluatie	1	0	2

De performance binnen bandbreedte (ondermaats en bovenmaats)

De performance buiten de ondermaatse tolerantiegrens het risico is hoger dan gewenst.

De performance buiten de bovenmaatse tolerantiegrens; het risico is lager dan gewenst

BEDRIJFSPENSIOENFONDS
MOLENAARS
Stichting Molenaarspensioenfonds

Risicobereidheid en –tolerantie Reputatiemanagement (Risicohouding: kritisch)

	Risicobereidheidsprincipes		Risk Appetite indicator	streefwaarde	ondermaats <	bovenmaats >
1	Wij willen een goede relatie met deelnemers en met werkgevers	1	Cijfer tevredenheidsonderzoek onder deelnemers (schaal 1-10)	7	6	8
		1	Cijfer tevredenheidsonderzoek onder werkgevers (schaal 1-10)	7	6	8
2	Wij willen voldoen aan wet- en regelgeving en fraude voorkomen	2	Aantal boetes van toezichthouders	0	1	-1
3	Wij willen vertrouwen van en draagvlak bij stakeholders	3	Aantal klachten over kwesties die het vertrouwen raken van het fonds	0	1	-1
4	Het beloningsbeleid moet sober en uitlegbaar, maar wel kostendekkend zijn	4	Aantal keren afgekeurd beloningsbeleid door RvT	0	1	-1
5	Wij willen een positief imago in de pers	5	Aantal slechte media uitingen in de pers over ons fonds	0	1	-1

De performance binnen bandbreedte (ondermaats en bovenmaats)

De performance buiten de ondermaatse tolerantiegrens het risico is hoger dan gewenst.

De performance buiten de bovenmaatse tolerantiegrens; het risico is lager dan gewenst

Risicobereidheid en –tolerantie Producten en Regeling (risicohouding: kritisch)

Risicobereidheidsprincipes		Risk Appetite indicator	streefwaarde	ondermaats <	bovenmaats >
Wij willen een integere en beheerste bedrijfsvoering	1	Aantal boetes of aantekeningen m.b.t. integere en beheerste bedrijfsvoering	0	1	-1
Wij willen fondsdoucmenten die met elkaar in overeenstemming zijn	2	Aantal boetes of aantekeningen vanwege inconsistentie in fondsdocumenten	0	1	-1
Wij willen dat de uitvoering overeenkomt met de SLA en dat de monitoring daarvan een reflectie is van het contract	3	Aantal boetes of aantekeningen die te maken hebben met dit onderwerp	0	1	-1
Wij willen dat data integriteit en data betrouwbaarheid in relatie tot besluitvormingsprocessen adequaat en efficiënt zijn ingeregeld	4	Aantal tekortingkomingen in ISAE-rapporten door onze uitvoerders op IT en datamanagement	0	1	-1
Wij willen dat administratiepartijen met innovatieve betrouwbare systemen werken	5	IT en innovatiebudget als percentage van totale IT budget voor de uitbesteders	20%	19%	50%
Wij willen borgen dat onze uitvoerders dezelfde risicohouding hebben	6	Aantal partijen waarmee IRM Proces niet is afgestemd in 2017 ten aanzien van Risicohouding en Risicobereidheid	0	1	-1

De performance binnen bandbreedte (ondermaats en bovenmaats)

De performance buiten de ondermaatse tolerantiegrens het risico is hoger dan gewenst.

De performance buiten de bovenmaatse tolerantiegrens; het risico is lager dan gewenst

BEDRIJFSPENSIOENFONDS
MOLENAARS
Stichting Molenaarspensioenfonds

Risicobereidheid en –tolerantie Kapitaalmanagement (risicohouding: gebalanceerd)

	Risicobereidheidsprincipes
1	N.V.T.
2	Wij willen slechts beperkt afwijken van de strategische mix.
3	Wij hebben geen lange termijn visie op de richting van de rente of de valuta.
4	N.V.T.
5	Op lange termijn leveren beleggingen in zakelijke waarden een hoger verwacht rendement op dan obligaties.
6	Wij willen dat de beoordeling van beleggingen plaatsvindt aan de hand van zowel kwantificeerbare als kwalitatieve risico's.
7	Wij willen dat de beoordeling van beleggingen plaatsvindt aan de hand van zowel kwantificeerbare als kwalitatieve risico's.
8	Diversificatie is van belang voor het reduceren van risico's, maar daar zitten grenzen aan.
9	Diversificatie is van belang voor het reduceren van risico's, maar daar zitten grenzen aan.
10	Diversificatie is van belang voor het reduceren van risico's, maar daar zitten grenzen aan.
11	Diversificatie is van belang voor het reduceren van risico's, maar daar zitten grenzen aan.
12	Diversificatie is van belang voor het reduceren van risico's, maar daar zitten grenzen aan.
13	Wij hebben geen lange termijn visie op de richting van de rente of de valuta.
14	Wij willen dat het gebruik van derivaten primair gericht is op het reduceren van risico's.
15	Wij willen niet zelf beleggen.

	Risk Appetite indicator	streefwaarde	Aandacht	ondermaats <
1	Actuele dekkingsgraad	> VEV	<VEV	<MVEV
2	Feitelijke beleggingsmix tov mandaat	ja	aandacht	nee
3	Ex-ante renteafdekking	56%-64%	55%-56%, 64%-65%	<55%, >65%
4	Ex-post renteafdekking	n.v.t.	n.v.t.	n.v.t.
5	Inflatierisico - delta	=< 0 bps	0-5 bps	>5 bps
6	Volatiliteitsrisico - vrw	<110	110-150	>150
7	Volatiliteitsrisico - aandelen	<30	30-40	>40
8	Kredietrisico - IG portefeuille	>90%	80%-90%	<80%
9	Tegenpartij Derivaten - rating	>BBB	BB	<B
10	Concentratierisico - vrw landen	<65%	65%-80%	>80%
11	Concentratierisico - aandelen landen	<65%	65%-80%	>80%
13	Concentratierisico - totale portefeuille	<65%	65%-80%	>80%
14	Valuta	>85%	75%-85%	<75%
15	Securities lending - collateral	>102%	100%-102%	<100%
16	Uitbesteding, overschrijding	Nee	n.v.t.	Ja

De performance binnen bandbreedte

De performance behoeft aandacht

De performance buiten de ondermaatse tolerantiegrens het risico is hoger dan gewenst.

3.3. Stap 3: Identificeren en benoemen van risico's

Risico's zijn gebeurtenissen die het behalen van de doelstellingen van het fonds in de weg kunnen staan. Daarbij wordt onderscheid gemaakt naar strategische en operationele risico's. De operationele risico's en de beheersing daarvan worden afgestemd op de strategische risico's en beheersing daarvan.

Strategische risico's
Dit zijn de risico's die het realiseren van de strategische doelstellingen in de weg kunnen staan. Het identificeren en/of valideren van de strategische risico's is integraal onderdeel van de strategische (risico-)managenent cyclus. Het bestuur identificeert, definieert en actualiseert ten minste jaarlijks zijn strategische risico's en bij wijzigingen in missie, visie, strategie en/of strategische doelstellingen.

Ook bij significante wijzigingen in omgevingsfactoren en/of in de organisatie evalueert het bestuur de strategische risico's.

Bij de identificatie en definitie van de risico's beschrijft het fonds de risico's zo specifiek mogelijk in termen van oorzaak, onzekerheid en gevolg (voor de strategische doelstellingen). De uitvoering van de strategische risicoanalyse kan aanleiding zijn voor het bestuur om voor een bepaald jaar aanvullende risicothema's vast te stellen.

Het bestuur heeft de volgende strategische risico's gedefinieerd en vastgesteld.

Strategisch risico 1	**Veranderende wet- en regelgeving**
Door veranderende wet- en regelgeving (de verplichtstelling verdwijnt) kan het pensioenlandschap drastisch veranderen. Hierdoor ontstaat het risico dat aangesloten ondernemingen vertrekken bij MPF met als gevolg dat de continuïteit van MPF in gevaar komt.	
Strategisch risico 2	**Krimpende sector**
doordat de sector graanbewerking en graanverwerkende industrie krimpt, bestaat het risico dat de nieuwe toestroom van deelnemers lager wordt met als gevolg hogere kosten.	
Strategisch risico 3	**Uitbesteding**
Door de uitbesteding van werkzaamheden, waaronder de uitvoering van de pensioenregeling die per 1 januari 2017 van Syntrus Achmea is overgedragen aan AGH, bestaat het risico dat uitbestedingspartijen fouten maken die voor MPF kunnen leiden tot (1) imagoschade, (2) verlies van data integriteit, (3) financiële schade en (4) verhoogd niveau van toezicht door de toezichthouder.	
Strategisch risico 4	**Cyberrisico**
Doordat de intensiteit van aanvallen van buitenaf toeneemt, bestaat het risico dat dataverlies of beschadiging ontstaat. Het fonds kan dan worden geconfronteerd met datalekken, ontevreden deelnemers, reputatieschade en wellicht een continuïteitsrisico.	
Strategisch risico 5	**Verandervermogen bestuurders**
Doordat het pensioenlandschap verandert, bestaat het risico dat bestuurders alle veranderingen niet kunnen bijbenen en te veel in de oude situatie blijven hangen. Hierdoor ontstaat het risico dat bestuurders niet 'in control' zijn.	
Strategisch risico 6	**Verandervermogen uitvoerders**
Doordat het pensioenlandschap verandert, bestaat het risico dat uitvoerders alle veranderingen niet kunnen bijbenen en hun systemen niet op orde hebben. Het fonds kan worden geconfronteerd met fouten in de administratie, ontevreden deelnemers en reputatieschade.	
Strategisch risico 7	**Rente- en marktontwikkelingen**
Door rente- en marktontwikkelingen bestaat het risico dat de dekkingsgraad van het pensioenfonds daalt, omdat het rendement dat behaald wordt op de beleggingen achter blijft bij het vereiste eigen vermogen.	

Eigen Risicobeoordeling
Ten minste eens per 3 jaar voert het fonds een Eigenrisicobeoordeling (ERB) uit. De ERB is een proces dat uitmondt in een document dat een beschrijving geeft van het risicoprofiel van het fonds, een beoordeling van de financieringsbehoeften en een beoordeling van de risico's rondom indexatie. Het wettelijk kader voor de ERB is artikel 18b van het Besluit financieel toetsingskader pensioenfondsen.

De ERB zal minimaal eens in de 3 jaar worden uitgevoerd en opgesteld, tenzij er sprake is van een strategische risicotrigger. Dan zal het fonds eerder een ERB uitvoeren. De frequentie van 3 jaar sluit aan bij de frequentie waarmee het fonds een ALM-studie uitvoert op basis waarvan het strategisch beleid wordt bepaald. In het kader van efficiëntie wordt de ERB opgesteld in samenhang met elke ALM-studie.

Bij de uitvoering van de ERB wordt waar mogelijk gesteund op het bestaande risicomanagement raamwerk van het fonds, zoals beschreven in dit beleid.

Het bestuur gebruikt de uitkomsten van de ERB vanaf het moment dat deze beschikbaar zijn, bij de (strategische) besluitvorming. De governance, de kaders en het proces van de ERB zijn nader uitgewerkt in het ERB-beleid.

Operationele risico's
Dit zijn de risico's die het nakomen de operationele doelstellingen van het fonds in de weg kunnen staan. Het fonds onderkent qua operationele risico's de volgende categorieën.

Operationele risicocategorieën		
Financiële risico's		RAVC©-domein
1.	Verzekeringstechnische risico's	Kapitaalmanagement
2.	Matching en rente risico	Kapitaalmanagement
3.	Marktrisico	Kapitaalmanagement
4.	Kredietrisico	Kapitaalmanagement
Niet-financiële risico's		RAVC©-domein
5.	Operationele risico's	Producten en uitbesteding
6.	Uitbestedingsrisico's	Producten en uitbesteding
7.	IT-risico's	Producten en uitbesteding
8.	Integriteitsrisico's	Reputatiemanagement
9.	Juridische risico's	Besturingsfilosofie
10.	Omgevingsrisico's	Producten en uitbesteding
11.	Communicatierisico's	Reputatiemanagement
12.	Sponsorrisico	

Keten-risico-analyse
Voor de identificatie van de operationele risico's voert het fonds minimaal jaarlijks een keten-risico-analyse uit op de voornaamste procesketens. Gezien de eindverantwoordelijkheid van het fonds voor de integere en beheerste bedrijfsvoering van de activiteiten van het fonds, ongeacht of deze zijn uitbesteed, voert het fonds deze integraal uit.

Om meer inzicht te krijgen in de bedrijfsvoering van het fonds is een proceshuis opgesteld waarin de hoofd- en subprocessen van het pensioenfonds zijn vastgelegd en gecategoriseerd in besturende-, primaire- en secundaire processen. Uiteindelijk moet dit bijdragen aan beheerste en integere bedrijfsvoering waarbij het bestuur 'in control' is. Om dat doel te bereiken stellen we drie vragen:

1) Wat zijn de belangrijkste processen in het fonds? Dit resulteert in een overzicht van de processen.

2) Wat is het doel van de processen? Dit resulteert in een doelstelling per proces.

3) Hoe weet het bestuur dat de processen beheerst en integer zijn, in termen van doeltreffendheid en risicobeheer? Dit resulteert in performance en risk indicatoren per proces. Die moeten worden geborgd in de rapportagecyclus: de SLA met uitvoerders; rapportages door uitvoerders; monitoring door het fonds. Deze borging resulteert in beheerste en integere bedrijfsvoering waarbij het bestuur 'in control' is.

Door deze vragen te beantwoorden wordt het bestuur in staat gesteld:

- Overzicht te hebben in de processen van het fonds en de samenhang daarin;
- richting te geven aan de processen (doelbepaling en kaderstelling voor een beheerst en integer proces);
- een referentiekader te hebben voor de afspraken met uitvoerders in contracten en SLA's;
- een referentiekader te hebben voor de monitoring van de rapportages die het fonds van de uitvoerders ontvangt.

Hierbij hanteert het fonds het proces-model zoals hieronder opgenomen.

<table>
<tr><td colspan="8">Onze Legitimiteit - Sociale Partners - Sponsor</td></tr>
<tr><td>Van strategie naar operationalisatie</td><td colspan="6">Wij zijn Pensioenfonds MPF</td><td>Planning & Control Cyclus</td></tr>
<tr><td>Besturende processen - Van Strategie tot Besturing</td><td colspan="6">Strategie - Leiderschap - Besluitvorming – Stakeholder- en toezichtmanagement</td><td>Eén keer jaar</td></tr>
<tr><td>Primaire processen - Van Registratie tot Communicatie</td><td>Markt- en sector ontwikkelingen</td><td>Deelnemers-administratie</td><td>Werkgevers-administratie</td><td>Beleggingen (investment)</td><td>Uitkeringen aan deelnemers</td><td>Communicatie</td><td>Constante cyclus</td></tr>
<tr><td rowspan="7">Secundaire processen - Van Administratie tot Waarde creatie</td><td colspan="5">Actuariaat</td><td rowspan="7">Constante cyclus</td></tr>
<tr><td colspan="5">Financiële administratie fonds</td></tr>
<tr><td colspan="5">Risk & Compliance</td></tr>
<tr><td colspan="5">Leveranciersmanagement in de keten</td></tr>
<tr><td colspan="5">Informatie technologie</td></tr>
<tr><td colspan="5">Bestuurszaken (aan de bestuurstafel)</td></tr>
<tr><td colspan="5">Audit Management</td></tr>
</table>

In het model worden 3 categorieën van processen onderscheiden:

- **Besturende processen**: de processen die (strategische) richting geven aan de primaire processen, gebaseerd op de regeling die is afgestemd door sociale partners en de opdrachtaanvaarding door het bestuur.
- **Primaire processen**: de kernprocessen van het fonds die het aanbod van producten en diensten aan de deelnemers en werkgevers kenmerkt.
- **Secundaire processen**: de processen die de primaire processen operationeel faciliteren door ze te ondersteunen en te controleren.

Thematische risico analyses
In aanvulling op keten-risico-analyses voert het bestuur van het fonds periodiek risicoanalyses uit op specifieke thema's. Bij de bepaling van de thema's en de frequentie laat het fonds zich leiden door haar initiële risico-inschatting en/of de vereisten uit wet- en regelgeving. Ook voor de thematische risico-analyses geldt dat deze worden uitgevoerd door de gehele procesketen van het fonds.

Het fonds onderscheidt de volgende thematische risico analyses:

- De Systematische integriteitsrisicoanalyse (SIRA) – minimaal jaarlijks.
- IT – en cybersecurity risicoanalyse (databeveiling) – minimaal eens per 2 jaar.
- Privacy (AVG compliance, keten in verwerkingsregister) – minimaal eens per 2 jaar.
- Cloudcomputing – eenmalig en daarna steeds per wijziging.
- Uitbesteding en contractmanagement – eens per 2 jaar.
- Verandervermogen bestuur en uitvoerders – eens per jaar.

Het integriteitsrisico is één van de (hoofd-)risicocategorieën die in het risicobeleid is onderkend. Dit betekent dat het integriteitsrisico een integraal onderdeel is van het jaarlijks risico identificatie proces en dat dit risico integraal zal worden behandeld bij voorstellen aan het bestuur. Beleid omtrent integriteitsrisico's is in een apart document; 'het integriteitsbeleid' opgenomen.

Voor de vastlegging van de strategische en operationele risico's en het eigenaarschap (en de beheersmaatregelen, zie stap 4 en verder) hanteert het fonds risico-control matrices.

4. Risico processen

In hoofdstuk drie is het stappenplan aangegeven. Nu dit vast staat dienen de uitkomsten uit dat stappenplan, geïmplementeerd te worden. Dit wordt gedaan in dit kwadrant. De vastgestelde risicohouding, risicobereidheid en de identificatie van de risico's is de basis voor de doorlopende processen voor de evaluatie, beheersing, bewaking en bijsturing. De kaders daarvoor worden onder stap 4 tot en met stap 8 nader uitgewerkt.

4.1. Stap 4: Wegen van risico's

Na identificatie van de risico's wordt een inschatting gemaakt van de bijbehorende kans en impact die te verwachten is als er geen beheersmaatregelen worden ingezet. De combinatie van de scores op kans en impact levert het zogenaamde 'bruto risico' op.

- **Kans:** weging van de mogelijkheid dat een gebeurtenis plaatsvindt.
- **Impact:** weging van de mate waarin het risico, indien het zich voordoet, invloed heeft op de realisatie van doelstelling(en).
- **Bruto risico:** uitkomst van de vermenigvuldiging van de weging van de kans en de weging van de impact (ten opzichte van te realiseren doelstelling(en)), zonder de inzet van beheersmaatregelen.

De inschattingen van kans en impact van het risico worden bepaald op onderstaande vijfpuntsschaal:

Kans	Kans (niet-) financieel	Impact	Impact financiële risico's	Impact niet-financiële risico's
1. Zeer gering	Onwaarschijnlijk dat het zich voordoet de komende 5 jaar/ Heeft zich niet eerder voorgedaan binnen het fonds.	1. Zeer gering	Dekkingsgraad wordt niet negatief beïnvloed.	Risico op interne negatieve of kritische berichtgeving (incl. uitvoerders)/ Het niveau van dienstverlening van het fonds wordt beïnvloed, maar geen gevolgen voor de tevredenheid van deelnemers/ Makkelijk te herstellen.
2. Laag	Doet zich mogelijk voor binnen 3 jaar/ Heeft zich voorgedaan de afgelopen 5 jaar.	2. Laag	Dekkingsgraad daalt met maximaal 5%/ Dekkingsgraad daalt onder 110%.	Risico op interne negatieve of kritische berichtgeving (incl. uitvoerders)/ Het niveau van dienstverlening van het fonds wordt beïnvloed, met als gevolg een beperkte daling van de tevredenheid van deelnemers/ Is te herstellen.
3. Middel	Heeft de potentie om op te treden binnen het komend jaar/ Heeft zich voorgedaan de afgelopen 2 jaar.	3. Middel	Dekkingsgraad daalt met maximaal 10%/ Dekkingsgraad daalt onder 105%.	Risico op negatieve publiciteit pensioensector/ Negatieve reacties vanuit DNB of AFM/ Het niveau van dienstverlening van het fonds wordt beïnvloed, met als gevolg een behoorlijke daling van de tevredenheid van deelnemers/ Is moeilijk te herstellen.
4. Hoog	Treedt op het komend jaar/ Heeft zich het afgelopen jaar voorgedaan.	4. Hoog	Dekkingsgraad daalt met meer dan 10%/ Dekkingsgraad daalt onder 100%.	Risico op negatieve publiciteit pensioensector/ Structureel negatieve reacties vanuit DNB of AFM of AP/ Het niveau van dienstverlening van het fonds wordt beïnvloed, met als gevolg een grote daling van de tevredenheid van deelnemers/ Erg moeilijk te herstellen.
5. Vrijwel zeker	Treedt op het komend half jaar/ Heeft zich het afgelopen 6 maanden voorgedaan.	5. Catastrofaal	Dekkingsgraad daalt met meer dan 15%/ Dekkingsgraad daalt onder 90%.	Risico op negatieve publiciteit richting pensioensector en aanverwante sectoren (werkgevers en werknemers)/ Aantekening of boete vanuit DNB of AFM of AP/ Het niveau van dienstverlening van het fonds wordt sterk beïnvloed, met als gevolg een zeer grote daling van de tevredenheid van deelnemers/ Bijna niet meer te herstellen.

4.2. Stap 5: Beheersmaatregelen en netto risico's

Het bestuur van het fonds heeft meerdere opties om met risico's om te gaan, de zogenaamde reactie op het risico of 'risk-response'. De verschillende risk-responses zijn:

- *Accepteren* (er worden geen extra maatregelen genomen).
- *Vermijden* (de activiteit waaraan het risico verbonden is wordt niet (meer) uitgevoerd of er wordt een ander besluit genomen).
- *Overdragen* (zoals (her-)verzekeren en hedgen).
- *Beheersen* (treffen van maatregelen om de impact of de kans te beperken).

De keuze voor de risk-response bepaalt het bestuur op basis van de hoogte van het (bruto) risico ten opzichte van de risicobereidheid, het karakter van het risico en de kosten die met de keuze voor de risk-respons samenhangen. De gekozen respons en bijbehorende maatregelen (indien van toepassing) hebben tot doel de kans en/of de impact van het risico te verlagen.

De verwachte invloed van de beheersmaatregelen op de kans en/of impact van het betreffende risico wordt vastgesteld en levert een zogenaamd 'netto risico' op: het bruto risico met aftrek van het effect van de maatregelen. Bij de weging van de netto risico's hanteert het fonds dezelfde criteria als voor de bruto risico's.

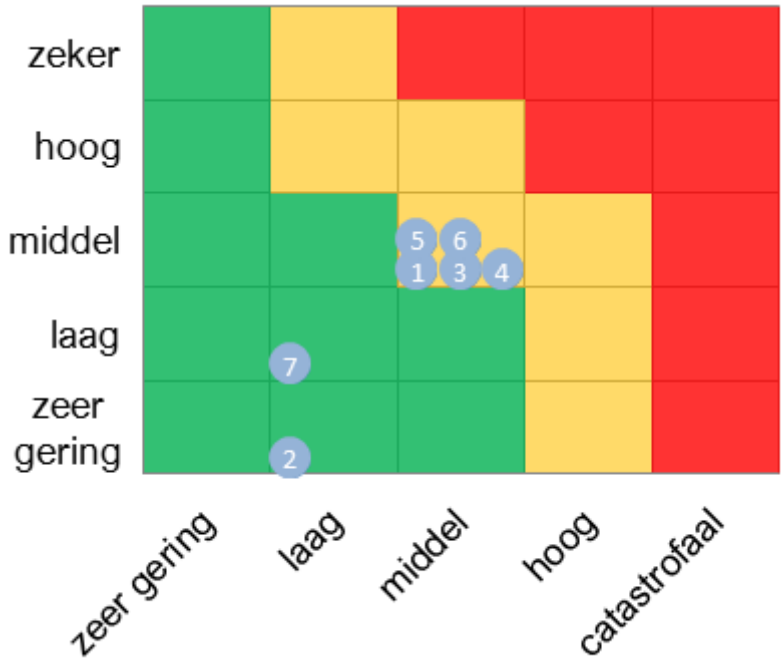
De risk-response, de bijbehorende maatregelen en de weging van het netto-risico worden vastgelegd in de risico-control-matrices. De opzet (beheers-)maatregelen worden zo specifiek (SMART) mogelijk beschreven zodat eenduidig is vast te stellen of de beheersmaatregel bestaat en werkt.

Voor de grafische weergave van de (relatieve) inschatting van de weging van de risico's (zowel bruto en netto) hanteert het fonds een heatmap (een voorbeeld is opgenomen in bijlage b1.5). De positie van het risico wordt bepaald door enerzijds de inschatting van de impact en anderzijds de kans. De kleuring in de heatmap is in drie kleuren: Rood, Oranje en Groen. De kleuren geven de zwaarte van het risico aan. Samen met de positionering van het risico in de heatmap, bepaalt dit de basis voor de reactie op het risico (zie stap 5).

De weging van de bruto risico's voor zowel strategische als operationele risico's dient minimaal jaarlijks te worden geëvalueerd.

Onderstaand wordt de heatmap getoond van de strategische risico's zoals deze zijn vastgesteld door het bestuur.

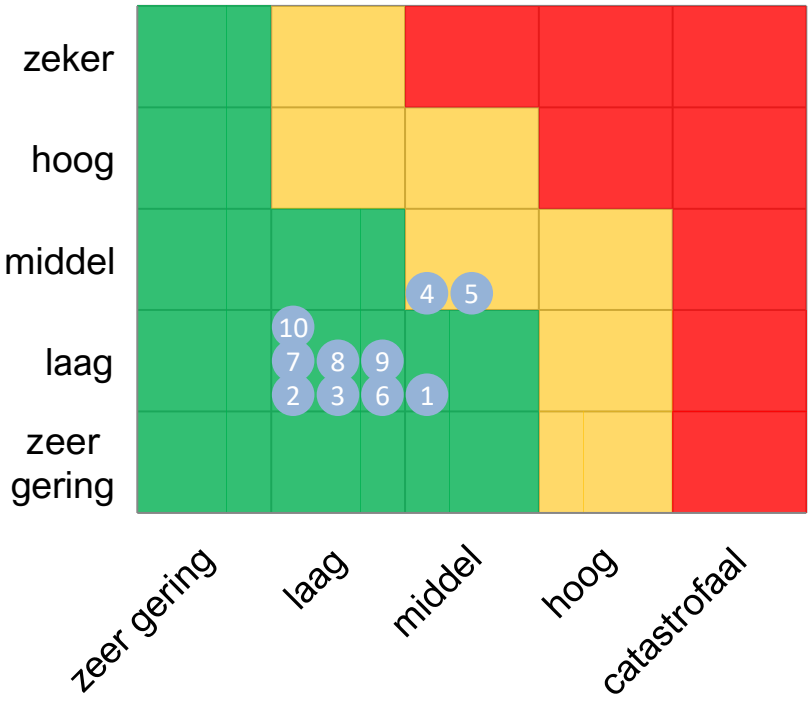
Heatmap strategische risico's



Strategische risico's	
#	**Omschrijving**
1	Veranderende wet- en regelgeving
2	Krimpende sector
3	Uitbesteding
4	Cyberrisico
5	Verandervermogen bestuurders
6	Verandervermogen uitvoerders
7	Rente- en marktontwikkelingen

Netto risico

Heatmap van de operationele risico's



Operationele risico's	
#	**Omschrijving**
1	Omgevingsrisico
2	Communicatierisico
3	Operationeel risico
4	Uitbestedingsrisico
5	IT-risico
6	Juridisch risico
7	Integriteitsrisico
8	Matching-/renterisico
9	Derivatenrisico
10	Kredietrisico

Netto risico

4.3. Stap 6: Borgen van beheersmaatregelen in de organisatie

In deze stap staat het borgen van de beheersmaatregelen in de organisatie centraal. Het bestuur borgt dat de gekozen en gedocumenteerde beheersmaatregelen daadwerkelijk zijn ingericht ('bestaan') en dat deze ook effectief werken ('werking'). Daarvoor wijst het bestuur eigenaarschap van de beheersmaatregelen toe aan commissies en/of het bestuursbureau of externe adviseur.

Het bestuur en de commissies borgen de werking van de maatregelen onder meer door deze op te nemen in de jaarkalender van de commissie en in de afspraken met uitbestedingpartijen.

De IRM-commissie adviseert het bestuur en de commissies over de maatregelen, de uit te voeren risicoanalyses en de overige risicomanagementactiviteiten. Daarvoor stelt de IRM-commissie jaarlijks een IRM-jaarplan op. Na afstemming met de commissie wordt deze door het bestuur vastgesteld. Door opname van de activiteiten uit het IRM-jaarplan in de jaarkalender van het bestuur en de commissies geven zij hieraan concreet invulling.

4.4. Stap 7: Informeren en communiceren

4.4.1 Uitdragen van het risicomanagement beleid

Om ervoor te zorgen dat draagvlak ontstaat voor de principes en consequenties van risicomanagement, communiceert het bestuur het risicomanagementbeleid en de daarmee corresponderde uitkomsten naar de verschillende organen binnen het fonds, de uitbestedingsrelaties en andere stakeholders.

De communicatie is erop gericht dat ieder zijn verantwoordelijkheid in het risicomanagementproces heeft en neemt. Bovendien is de communicatie erop gericht informatie te verzamelen die nodig is om de dialoog over het risicomanagement-raamwerk te versterken, en hierdoor het risico bewustzijn binnen het fonds verder toe te snijden op de fondsspecifieke situatie.

Het bestuur draagt het IRM-beleid uit door ten minste de volgende activiteiten.

- Het beleid wordt geborgd in het strategiedocument/de ABTN en via de reguliere kanalen gecommuniceerd en ter beschikking gesteld aan stakeholders.
- Bij de evaluatie en actualisering van het IRM-beleid wordt explictiet afgestemd met de commissies en met de uitvoeringspartijen. Na de vaststelling van het IRM-beleid worden de aanpassingen besproken in de eerstelijnscommissies, in het bijzijn van een vertegenwoordiger van de risicomanagementfunctie.
- Jaarlijks stelt IRM-commissie, in afstemming met eerstelijnscommissies, het IRM-jaarplan op. Dit wordt na vaststelling zo nodig in het bestuur toegelicht in de eerstelijnscommissies.
- Het IRM-beleid en het IRM-jaarplan worden door de sleutelfunctiehouder risicomanagement besproken met de Raad van Toezicht.
- Minimaal twee maal per jaar rapporteert de sleutelfunctiehouder risicomanagement over de voortgang en de resultaten van het IRM-jaarplan aan het bestuur en de Raad van Toezicht.
- Het IRM-beleid, IRM-jaarplan en overige beleidsstukken worden ter beschikking gesteld via Ourmeeting.
- Beleidsvoorstellen worden getoetst aan het risicoraamwerk. De voorlegger bij (voorgenomen) bestuursbesluiten kent een standaard indeling met een risicoparagraaf, waarin de indiener (de samenvatting van) de risicoanalyse opneemt en waar ruimte is voor de opinie van de (tweede lijns) risicomanagementfunctie.

- Uitkomsten van besluitvorming worden vastgelegd in notulen inclusief de onderbouwing van het besluit;
- Risicomanagement is een terugkerend agendapunt bij de bestuursvergadering.
- Bij de jaarlijkse zelfevaluatie van het bestuur en de commissies is de werking van het risicomanagement een vast onderwerp. Eventuele aandachtspunten worden meegenomen in evaluatie van IRM-beleid of leiden indien nodig tot directe aanpassing.
- Bij de jaarlijkse evaluatie van de uitbestedingspartners is de werking van het risicomanagement een vast onderwerp.
- Het verantwoorden van de mate van effectiviteit van het risicoraamwerk in het jaarverslag, waarbij ook wordt aangegeven op welke onderdelen het risicoraamwerk (verder) is aangepast en/of geoptimaliseerd aan de fondsspecifieke siutatie en de onderbouwing daarvan (conform RJ 400).
- Analyse van compliance aan code pensioenfondsen ten aanzien van IRM.

Het bovenstaande proces wordt zowel voor de strategische en de operationele cyclus doorlopen.

4.4.2 Informeren en rapporteren

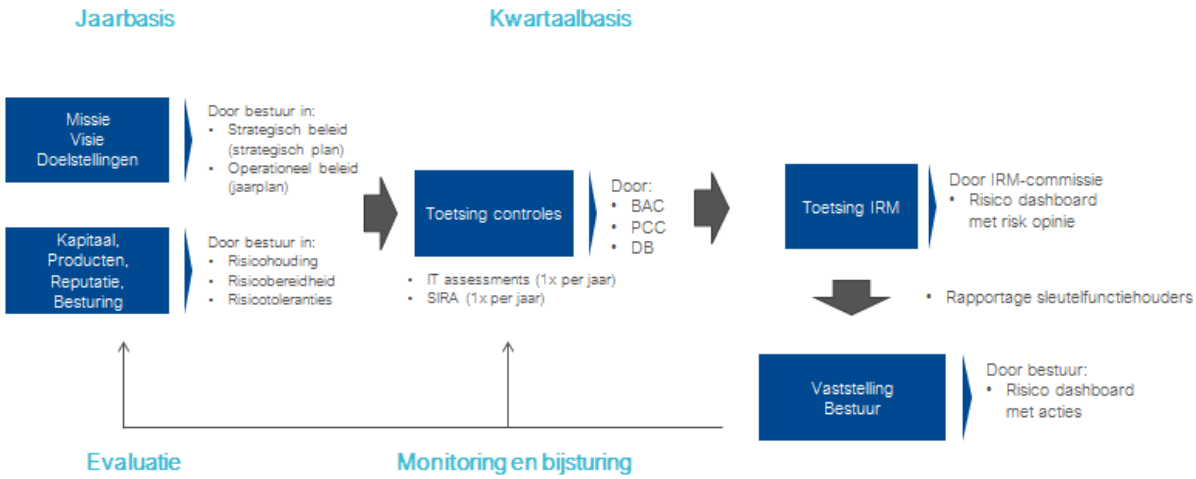
De effectiviteit van het risicomanagementbeleid wordt inzichtelijk aan de hand van rapportages over de beheersing van risico's. Door middel van de rapportagecyclus dient het bestuur in staat te zijn inzicht te hebben in het actuële (werkelijke) risicoprofiel van het fonds, daar waar nodig bij te sturen en zich over haar risicomanagement te kunnen verantwoorden. Voor de monitoring van de risico's en bijsturing van de risicobeheersing steunt het bestuur onder meer op de PCC en de BAC voor respectievelijk de pensioenbeheer- en vermogensbeheerketen. Deze commissies dienen elk voor haar domein inzicht te hebben in de risico's en de beheersing.

Het inzicht in de risico's wordt verkregen door de uitkomsten van de eerdere stappen in het proces.

Het fonds onderkent 3 niveaus van informatievoorziening

1. Het risico dashboard (bestuur en commissies): het integrale inzicht in het actuele risicoprofiel en de ontwikkeling daarin (strategische en operationele risico's, zowel financieel als niet-financieel), de risico's die aandacht behoeven en (voorgestelde) aanvullende maatregelen en een opinie en aanbevelingen van (tweede lijns) risicomanagement.
2. Analyse (door IRM-commissie op basis van niveau 3) overzicht en inzicht in de status van de risk appetite indicatoren, effectiviteit van de risicobeheersing, de (risicomanagement-)acties en incidenten.
3. Bronrapportages en documentatie (commissies): Achterliggende deelrapportages en detail-overzichten die ten grondslag liggen aan de analyse, waaronder rapportages van uitbestedingspartijen.

Uitwerking risicobeheercyclus MPF



4.5. Stap 8: Monitoren en evaluatie van het gehele proces en reflectie Monitoring (bewaking).

Monitoring en evaluatie van het risicomanagementproces wordt minimaal jaarlijks uitgevoerd. Door te reflecteren op de opzet, bestaan en werking van risicomanagement blijft de integere en beheerste bedrijfsvoering gewaarborgd en zal de effectiviteit continu verbeteren. Reflectie leidt, waar nodig, tot herijking van (onderdelen van) de bedrijfsvoering in het algemeen en risicomanagement in het bijzonder.

Tevens draagt dit bij aan het verhogen van het volwassenheidsniveau van het risico-management binnen het fonds.

Als uitkomst van de evaluatie wordt vastgesteld of het risicomanagement beleid dient te worden bijgesteld. Eventuele vastgestelde bijstellingen worden verwerkt in dit IRM-beleidsdocument.

5. Risico Bewustzijn

Het complementerende onderdeel in ons beleid is intrinsieke motivatie. De drie eerdere kwadranten zijn overbodig indien er geen intrinsieke bewustzijn is ten aanzien van IRM. Het risicobewustzijn is het 'in de genen hebben' van het risicomanagement in de gehele procesketen. Meer concreet is er sprake van risicobewustzijn binnen de organisatie als onder andere de volgende vragen bevestigend worden beantwoord:

Zijn we lerende mensen – hebben we een intrinsieke motivatie om risicomanagement beter te begrijpen en toe te passen?

Zijn we een lerende organisatie – worden processen van beleidsinrichting, monitoring, evaluatie en herijking goed doorlopen, met een intrinsieke motivatie om het proces te verbeteren?

Wordt risicomanagement en de (interne) communicatie daarover tijdig meegenomen in de Beeldvorming, Oordeelsvorming en Besluitvorming (BOB)?

Zijn de bestuursleden zich intrinsiek bewust van risico en rendement en hun leiderschap in dit proces (tone at the top)?

- Is de bestuursondersteuning en zijn onze uitbestedingsrelaties zich intrinsiek bewust van hun verantwoordelijkheid in dit proces?

- Is de risicohouding expliciet onderdeel van onze (duiding van) 'boardroom dynamics'?
- Hebben we een (risico)cultuur waarin wij:
  - onze gezamenlijke en eigen verantwoordelijkheid begrijpen en toepassen, en anderen faciliteren hun verantwoordelijkheid te nemen.
  - ons lerend vermogen aanspreken door reflectief te zijn richting onszelf en anderen, open staan voor elkaar, naar elkaar luisteren.
  - onze countervailing power ten opzichte van elkaar constructief en respectvol inzetten en ontvangen.

De beantwoording van deze vragen zijn onderdeel van de jaarlijkse evaluatie van het IRM raamwerk en de zelfevaluatie van het bestuur.

Het doorlopend uitvoeren van de risicomanagement processen en de activiteiten genoemd onder 4.4.1 dragen bij aan het vergroten van het risicobewustzijn bij het fonds en de uitbestedingspartners. Daarnaast adviseert de IRM-commissie jaarlijks over eventuele aanvullende activiteiten ter versterking van het risicobewustzijn. Deze worden opgenomen in het IRM-jaarplan.

6. Vaststelling

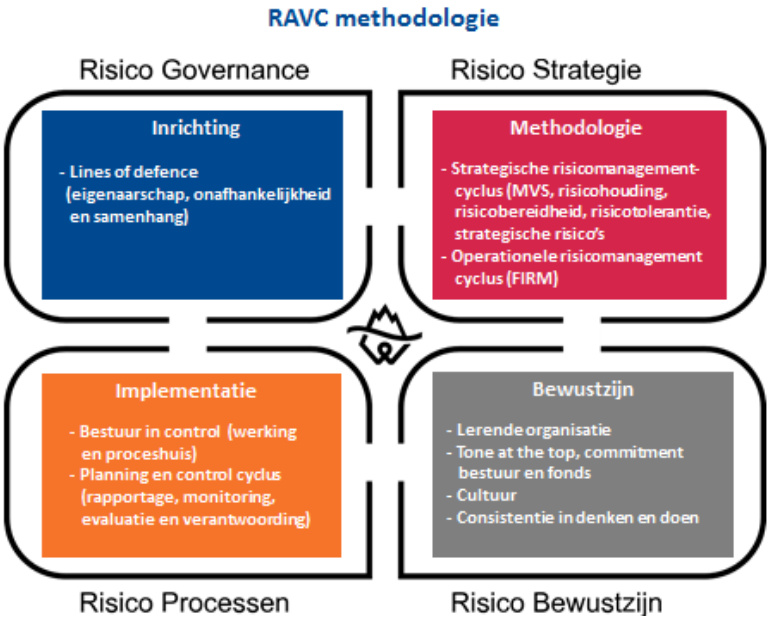
Dit document is vastgesteld door het bestuur van Stichting Molenaarspensioenfonds op 16 september 2019.

Mevrouw E. Bronswijk	De heer J. Teuwen
Voorzitter	Plaatsvervangend vicevoorzitter

Bijlage 1. Theorie ten grondslag aan beleid

B1.1 Het RAVC© vier kwadrantenmodel

Binnen het integraal risicomanagement raamwerk maken we onderscheid naar vier kwadranten. Deze kwadranten moeten in samenhang worden bezien. De elementen genoemd in deze kwadranten worden allen geborgd in het IRM-beleid.



Risico Governance
Bij risico governance staat de borging van het IRM-proces (eigenaarschap en vastlegging in beleid) binnen de governancestructuur van het fonds centraal, evenals de borging van countervailing power intern en richting de uitvoeringsorganisaties.

Risico Strategie
Risicomanagement is het managen van risico's die het behalen van de doelstellingen van het fonds in de weg kunnen staan. IRM stelt het fonds in staat om de missie, visie en doelstellingen te realiseren. Een duidelijke missie, visie, heldere doelstellingen en een passende en eenduidige risicohouding, risicobereidheid en risicotolerantie vormen de basis voor efficiënt en effectief IRM. Het fonds identificeert daarnaast de risico's die de strategische doelstellingen kunnen bedreigen. Samen vormt dit de Strategische Risicomanagementcyclus. Daarnaast is er een Operationele risicomanagementcyclus. Beide cycli zijn hieronder toegelicht.

Risico Processen
Dit kwadrant beschrijft op welke wijze het bestuur in control is en blijft, zowel in de strategische- als operationele risicomanagementcyclus en ten opzichte van besturende, primaire en secundaire processen. Door rapportage, monitoring en evaluatie van het risicoprofiel en de risicobeheersing wordt aantoonbare werking van risicomanagement gerealiseerd en waarde toegevoegd aan de bedrijfsvoering. Over het risicomanagement wordt ook verantwoording, intern en aan derden, afgelegd.

Risico Bewustzijn
Het risicobewustzijn is het 'in de genen hebben' van het risicomanagement in de gehele procesketen. Met de juiste tone at the top en risicocultuur waarin consistent wordt gehandeld kan een lerende organisatie ontstaan.

De Strategische besturingscyclus van risicomanagement: van opzet en bestaan naar werking door RAVC werk- en denkmodel

IRM besturingscyclus	De cruciale elementen	Waarom belangrijk	Documenten: waar dienen ze voor en hoe weten we dat we doen wat we hebben afgesproken?			
			Vaststelling beleid	**Werking realiseren**	**Monitoren en evalueren**	**Frequentie monitoring**
Strategische risicomanagement-cyclus: de missie, visie, strategie en strategische doelstellingen vertalen in een strategisch risicomanagement normenkader en strategische risico's beheersen	**Risicohouding**	Expliciteren van grondhouding ten aanzien van risico en rendement, volgens de classificatie Nul – Kritisch – Gebalanceerd – Opportuun – Maximaal. Deze schaal gaat geleidelijk van risicomijdend naar risico zoekend. Deze menskant van risicomanagement is fundamenteel voor besluitvorming- en besturingsprocessen	Integraal Risicomanagement-beleid; Risicomanagement-paragraaf in overige beleidsdocumenten	Voorlegger besluitvormings-processen; Jaarplan IRM-commissie	Risico-dashboard	Jaarlijks/ wijziging risicoprofiel
	Risicobereidheid	Geeft met principes uitdrukking aan wat het bestuur van waarde en belang acht. Het zijn de zgn. stoepranden waaraan beleid en uitvoering moeten voldoen. Risicobereidheid is daarmee van tevoren vastgelegd voor besluitvorming- en besturingsprocessen.	Integraal Risicomanagement-beleid; Risicomanagement-paragraaf in overige beleidsdocumenten	Voorlegger besluitvormings-processen; Proceshuis; Jaarplan IRM-commissie	Risico-dashboard	Jaarlijks/ wijziging risicoprofiel
	Risicotolerantie	Concretisering van risicobereidheidsprincipes, door normerende streefwaarden en grenzen te bepalen. Zogezegd de hoogte/dikte van stoepranden. Deze normeringen/ indicatoren zijn essentieel om concreet te toetsen of de uitvoering voldoet aan door het bestuur vastgestelde normering.	Integraal Risicomanagement-beleid	Voorlegger besluitvormings-processen; Proceshuis; Jaarplan IRM-commissie	Risico-dashboard	Jaarlijks/ wijziging risicoprofiel
	Scenariomanagement/ Eigen Risico Beoordeling (ERB – IORP II)	Inzicht in scenario's die effect kunnen hebben op (financiële en niet-financiële) risicoprofiel van het fonds.	Integraal Risicomanagement-beleid (ERB paragraaf)	Driejaarlijks/ n.a.v. trigger uitvoeren scenario-analyse/ ERB proces	Macro-economische ontwikkelingen bijhouden	Continue

IRM besturingscyclus	De cruciale elementen	Waarom belangrijk	Documenten: waar dienen ze voor en hoe weten we dat we doen wat we hebben afgesproken?			
			Vaststelling beleid	**Werking realiseren**	**Monitoren en evalueren**	**Frequentie monitoring**
	Strategische risico's	Inzicht in wat de belangrijkste gebeurtenissen zijn die impact hebben op de doelstellingen en strategie van het fonds.	Integraal Risicomanagement-beleid	Voorlegger besluitvormings-processen; Proceshuis; Jaarplan IRM-commissie	Risico assessment; Heatmap; Strategische Risico Control Matrix	Jaarlijks/ wijziging risicoprofiel
	Beheersmaatregelen	Beheersmaatregelen zijn (organisatorische-, technische-, gedrags-) interventies die er toe leiden dat de geïdentificeerde risico's worden beheerst binnen het normenkader van het bestuur, zodat de doelstellingen behaald kunnen worden. Er moet ook een proces zijn waarmee wordt toegezien op de effectiviteit van beheersmaatregelen.	Integraal Risicomanagement-beleid	Strategische Risico Control Matrix; RACI; Jaarplan IRM-commissie	Strategische Risico Control Matrix; Risico-dashboard	Jaarlijks/ wijziging risicoprofiel
	Externe transparantie	Alle belanghebbenden informeren over de wijze waarop beheerste en integere bedrijfsvoering wordt toegepast en nageleefd.	Integraal Risicomanagement-beleid	Risicoparagraaf Jaarverslag; Jaarplan IRM-commissie	Niet van toepassing	Jaarlijks

De Operationele besturingscyclus van risicomanagement: van opzet en bestaan naar werking door RAVC werk- en denkmodel

IRM besturingscyclus	De cruciale elementen	Waarom belangrijk	Documenten: waar dienen ze voor en hoe weten we dat we doen wat we hebben afgesproken?			
			Vaststelling beleid	Werking realiseren	Monitoren en evalueren	Frequentie monitoring
Operationele risicomanagement-cyclus: de operationele risico's beheersen in lijn met het strategisch risicomanagement normenkader	**Operationele risico's – FIRM**	De (interne en uitbestede) bedrijfsvoering in lijn brengen met het normenkader van het fonds en voldoen aan het normenkader van toezichthouder.	Integraal Risicomanagement-beleid;	Voorlegger besluitvormings-processen; Proceshuis; Risico assessment; Heatmap; Inrichting contracten en SLA conform normenkader; Jaarplan IRM-commissie	Risico assessment; Heatmap; Operationele Risico Control Matrix; ISAE; SLA rapportage; Risicorapportage; Incidentenrapportage; Gespreksverslag dialoog met uitvoerders	Afhankelijk type risico/trigger: per incident/ per maand/ per kwartaal/ halfjaarlijks/ per jaar
	Operationele risico's – SIRA	Integriteit is een belangrijke kernwaarde die nageleefd moet worden en voldoen aan normenkader toezichthouder.	Integraal Risicomanagement-beleid; Integriteitsbeleid Gedragscode	Voorlegger besluitvormings-processen; Proceshuis; Jaarplan IRM-commissie	Risico assessment; Heatmap; Operationele Risico Control Matrix; ISAE; SLA rapportage; Risicorapportage; Incidentenrapportage; Rapportage compliance officer Gespreksverslag dialoog met uitvoerders	Afhankelijk type risico/trigger: per incident/ per maand/ per kwartaal/ halfjaarlijks/ per jaar
	Operationele risico's – IT	IT is een steeds belangrijker onderdeel van de bedrijfsvoering en van belang voor	Integraal Risicomanagement-beleid;	Voorlegger besluitvormings-processen;	Risico assessment; Heatmap; Operationele Risico Control Matrix;	Afhankelijk type risico/trigger: per incident/ per

IRM besturingscyclus	De cruciale elementen	Waarom belangrijk	Documenten: waar dienen ze voor en hoe weten we dat we doen wat we hebben afgesproken?			
			Vaststelling beleid	**Werking realiseren**	**Monitoren en evalueren**	**Frequentie monitoring**
		verandervermogen gezien veranderend pensioenlandschap. Beheersing van IT systemen en processen is dus cruciaal.	IT beleid (inclusief cyberrisico's, privacy risico's)	Proceshuis; Vragenlijst IT; Cloud assessment; Jaarplan IRM-commissie	ISAE; SLA rapportage; Risicorapportage; Incidentenrapportage; Gespreksverslag dialoog met uitvoerders; Privacy Impact Analyse	maand/ per kwartaal/ halfjaarlijks/ per jaar
	Operationele risico's – BCM	Beheersing van continuïteit van bedrijfsvoering, bij mogelijke uitval van kritische processen.	Integraal Risicomanagement-beleid; IT beleid; BCM beleid; Crisisplan	Voorlegger besluitvormings-processen; Proceshuis; Jaarplan IRM-commissie Calamiteitenoefening	Risico assessment; Heatmap; Operationele Risico Control Matrix; ISAE; SLA rapportage; Risicorapportage; Incidentenrapportage; Gespreksverslag dialoog met uitvoerders; Business Impact Analyse (BIA)	Afhankelijk type risico/trigger: per incident/ per maand/ per kwartaal/ halfjaarlijks/ per jaar
	Beheersmaatregelen	Beheersmaatregelen zijn (organisatorische-, technische-, gedrags-) interventies die er toe leiden dat de geïdentificeerde risico's worden beheerst binnen het normenkader van het bestuur, zodat de doelstellingen behaald kunnen worden. Er moet ook een proces zijn waarmee wordt toegezien op de effectiviteit van beheersmaatregelen.	Integraal Risicomanagement-beleid; Integriteitsbeleid; IT beleid; BCM beleid	Operationele Risico Control Matrix RACI; Vragenlijst IT; Cloud assessment; SIRA; Jaarplan IRM-commissie	Operationele Risico Control Matrix, Risico-dashboard	Afhankelijk type risico/trigger: per incident/ per maand/ per kwartaal/ halfjaarlijks/ per jaar
	Transparantie vanuit uitvoerders	Uitvoerders moeten rapporteren over hun dienstverlening zodat het bestuur kan toetsen of het voldoet aan het normenkader van het fonds.	Integraal Risicomanagement-beleid; Integriteitsbeleid; IT beleid;	SLA rapportages; Incidentenrapportages; Risicorapportages; ISAE	Evaluatie uitvoerder; Gespreksverslag dialoog met uitvoerders, Risico-dashboard	Afhankelijk type risico/trigger: per incident/ per maand/ per kwartaal/

IRM besturingscyclus	De cruciale elementen	Waarom belangrijk	Documenten: waar dienen ze voor en hoe weten we dat we doen wat we hebben afgesproken?			
			Vaststelling beleid	Werking realiseren	Monitoren en evalueren	Frequentie monitoring
			BCM beleid; Uitbestedingsbeleid			halfjaarlijks/ per jaar

B1.2 COSO Enterprise Risk Model 2017

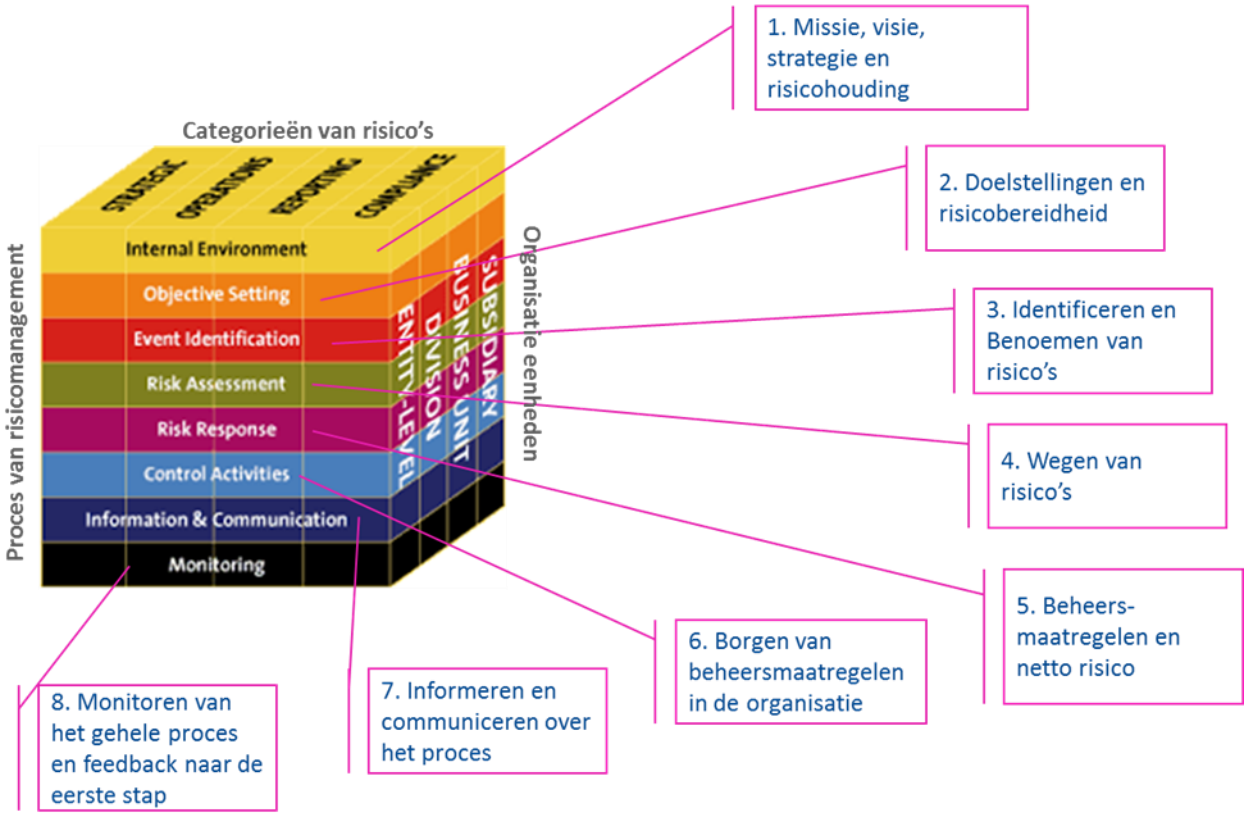
Het COSO Enterprise Risk Management model geldt als een standaard voor risicomanagement. In 2017 is het model vernieuwd. Om weg te blijven van een 'checklist' gevoel, zijn 20 principes geformuleerd die richting geven aan de toepassing van risicomanagement in een organisatie. Hieronder zijn deze 20 principes ondergebracht bij de vier RAVC kwadranten.

RAVC Kwadranten	Stappen COSO 2004	Principes COSO 2017
Governance: · Lines of defence · Eigenaarschap	Zijkant van de COSO kubus	1. Exercises Board Risk Oversight (bestuur monitort in hoeverre de bedrijfsvoering voldoet aan het (IRM) normenkader/risicoprofiel). 2. Establishes Operating Structures (inrichting van governance met eigenaarschap, rollen, verantwoordelijkheden, mandaten, bevoegdheden).
Strategie : · Strategische risicomanagement cyclus (MVS, risicohouding, risicobereidheid, risicotolerantie, strategische risico's) · Operationele risicomanagement cyclus (FIRM)	Stap 1. Missie, visie, strategie en risicohouding.	6. Analyzes Business Context (analyse van de interne governance en cultuur en daarnaast de omgeving, inclusief alle belanghebbenden en inclusief (onder)uitbesteding)). 7. Defines Risk Appetite (vaststellen van risicohouding (risk attitude) en risicobereidheid (risk appetite) en risicotolerantie (risk tolerance)). 8. Evaluate Alternative Strategies (bepalen van de strategie aan de hand van alternatieven, daarbij rekening houdend met missie, visie, risicohouding, risicobereidheid, risicotolerantie)
	Stap 2. De organisatiedoelstellingen en de risicobereidheid.	7. Defines Risk Appetite (vaststellen van risicohouding (risk attitude) en risicobereidheid (risk appetite) en risicotolerantie (risk tolerance)). 9. Formulates Business Objectives (bepalen van strategische en operationele doelstellingen, uitgewerkt in KPI (key performance indicators) en KRI (key risk indicators), opgenomen in contracten en SLA's (service level agreements) met uitvoerders).
	Stap 3. Het identificeren van risico's.	10. Identifies Risk (identificeren van strategische-, operationele-, en thematische risico's. Strategische risico's zijn risico's met impact op strategische doelstellingen, operationele risico's (FIRM) hebben impact op operationele doelstellingen, thematische risico's zijn detailrisico's op een bepaald thema zoals IT, BCM, integriteit).
Processen · Bestuur in control	Stap 4. Het wegen van (bruto) risico's.	11. Assesses Severity of Risk (bepalen van kans en impact van de geïdentificeerde risico's).

(werking en proces-huis)	Stap 5. Het bepalen en benoemen van beheersmaatregelen en het netto risico.	11. Assesses Severity of Risk (bepalen van kans en impact van de geïdentificeerde risico's) 12. Prioritizes Risks: The organization prioritizes risks as a basis for selecting responses to risks. *(prioritering van risico's op basis van risicohouding en risicobereidheid en kans en impact)* 13. Implements Risk Responses (bepalen en implementeren van beheersmaatregelen, inclusief eigenaarschap).
Processen · Planning en control cyclus (rapportage, monitoring, evaluatie en verantwoording)	Stap 6. Het borgen van de beheers-maatregelen in de organisatie.	13. Implements Risk Responses (bepalen en implementeren van beheersmaatregelen, inclusief eigenaarschap).
	Stap 7. Het informeren en communiceren over het proces.	18. Leverages Information and Technology (benutten van informatie en technologie om rapportages te kunnen maken, die hoogstaande stuurinformatie opleveren). 19. Communicates Risk Information (delen van informatie met mensen die werken voor de organisatie met als doel samen te leren; met belanghebbenden zoals deelnemers, toezichthouders met als doel te verantwoorden).
	Stap 8. Het monitoren van het gehele proces.	14. Develops Portfolio View (samenhang – correlatie en cumulatie – tussen verschillende risico's vaststellen en dit ook implementeren in de cyclus van rapportage, monitoring en evaluatie). 15. Assesses Substantial Change: The organization identifies and assesses changes that may substantially affect strategy and business objectives. *(identificeren van substantiële veranderingen/triggers waardoor Eigen Risicobeoordeling (ERB) moet worden uitgevoerd dan wel herijkt).* 16. Reviews Risk and Performance (werken met risicoparagraaf en risico-opinie in besluitvormingsproces). 18. Leverages Information and Technology (benutten van informatie en technologie om rapportages te kunnen maken, die hoogstaande stuurinformatie opleveren). 20. Reports on Risk, Culture, and Performance (uitvoeren van reguliere cyclus van rapportage, monitoring en evaluatie van (status van en incidenten in) bedrijfsvoering - rapportages bevatten zowel elementen van risico (risicohouding, risicobereidheid, risicotolerantie (RAI), KRI) en performance.
Bewustzijn: · Lerende organisatie · Tone at the top, commitment · bestuur en fonds · Cultuur	Stap 1. Risicocultuur.	3. Defines Desired Culture (cultuur creëren waarin de bedrijfsvoering in lijn met het beleid, waaronder IRM, wordt uitgevoerd). 4. Demonstrates Commitment to Core Values (gecommitteerd aan kernwaarden en uitgangspunten van (IRM)beleid)).
	Stap 8. feedback naar de eerste processtap, zodat een lerende organisatie ontstaat.	17. Pursues Improvement in ERM (leervermogen in de organisatie nastreven en realiseren).

· Consistentie in denken en doen		

Het COSO Enterprise Risk Management model 2004 (dus voor de update van 2017) bestaat uit acht stappen (aan de voorkant van de kubus). Deze stappen hebben betrekking op categorieën van risico's (de bovenkant van de kubus) en op organisatie eenheden (de zijkant van de kubus).



In het kort komen de processtappen in de Risk & Control cyclus op het volgende neer:

1. **Internal Environment (interne omgeving)**. Hier staat de formulering/de herijking van de missie, visie, strategie en risicohouding centraal.
2. **Objective Setting (formuleren van doelstellingen)**. Hier staan onze strategische doelstellingen en risicobereidheid centraal.
3. **Event Identification (identificeren van gebeurtenissen)**. Hier staat het identificeren en benoemen van risico's centraal.
4. **Risk Assessment (risicobeoordeling)**. Hier staat het wegen van (bruto) risico's centraal.
5. **Risk response (reactie op risico).** Hier staat het bepalen of risico's geaccepteerd of gemitigeerd worden en benoemen van beheersmaatregelen en het netto risico centraal.
6. **Control Activities (beheersingsactiviteiten)**. Hier staat het borgen van de beheersmaatregelen in de organisatie centraal.
7. **Information & Communication (informatie en communicatie)**. Hier staat het informeren en communiceren over het proces centraal.
8. **Monitoring (bewaking)**. Hier staat het monitoren van het gehele proces en feedback naar de eerste processtap centraal (zodat een lerende organisatie ontstaat).

Tevens is het van belang om de opzet, het bestaan en de werking van risicomanagement in verschillende eenheden van de organisatie te borgen.

Organisatie eenheden
Het COSO ERM model maakt onderscheid tussen eenheden in de organisatie:

- **Entity level**
  De organisatie als geheel. Het bestuur acteert, in samenspel met de totale governance, als regiehouder.
- **Division**
  De (staf)afdelingen binnen de organisatie. Dit is bijvoorbeeld de commissiestructuur binnen het pensioenfonds.
- **Business units**
  De (lijn)afdelingen binnen de organisatie. Dit is bijvoorbeeld het pensioenbureau.
- **Subsidiary**
  Letterlijk 'dochtermaatschappij'. Dit zijn de uitbestedingsrelaties.

B1.3 Risicohouding, risicobereidheid, risicotolerantie: resultanten van het RAVC© model

De eerste drie processtappen van het risicoraamwerk worden doorlopen met behulp van een gestructureerd werk- en denkmodel namelijk het Risk Appetite Value Chain model© (RAVC©). Dit model geeft handvatten om, aan de hand van de missie, visie, kernwaarden en strategie als vertrekpunt, de risicohouding, risicobereidheid en risicotolerantiegrenzen consistent, samenhangend en doeltreffend vast te stellen.

De risk appetite van het bestuur is kaderstellend voor de inrichting en besturing van de interne organisatie en haar uitvoerders. Het bepaalt de mate van organisatiebeheersing die noodzakelijk is voor een beheerste en voorspelbare realisatie van strategische doelen en vormt hiermee voor de deelnemers van het fonds een fundament. Het fundamentele referentiekader van het RAVC model zijn de vier kwadranten zoals in bijlage B.1.1. beschreven.

Strategisch proces: kansen en risico's
Het onderdeel 'strategisch proces: kansen en risico's' van de figuur geeft weer dat er, vanuit de missie, visie en kernwaarden, (financiële en niet-financiële) strategische doelstellingen van het fonds worden geformuleerd. Het bereiken van deze doelstellingen wordt echter bedreigd door risico's die optreden. Deze risico's moeten worden geïdentificeerd, beoordeeld en door het treffen van beheersmaatregelen geheel of gedeeltelijk worden gemitigeerd. De beheersmaatregelen worden ingebed in de Planning en Control cyclus. Dit gebeurt in de hierna volgende processtappen van het risicomanagement.

Risicohouding, risicobereidheid en risicotolerantie – RAVC© denken
Om te kunnen beoordelen of de borging en het effect van deze maatregelen leidt tot een acceptabele situatie, bepaalt het bestuur zijn risicobereidheid. Het denkproces begint bij het vaststellen van de risicohouding gevolgd door het vaststellen van de risicobereidheid en risicotolerantiegrenzen. De confrontatie tussen enerzijds de risk appetite en anderzijds de overgebleven 'netto' risico's en de monitoring van de risicobeheersing vindt plaats aan de hand van periodieke rapportages.

Om te komen van de risk appetite (ex-ante) naar een 'in control' verklaring (ex-post) worden onderstaande stappen uitgevoerd:

a) Implementeren van de risk appetite in beleidsstukken op strategisch en tactisch niveau.
b) De risk appetite vanuit het strategische en tactische niveau doorvertalen naar operationeel niveau door het aanwijzen van (key-)risico's en (key-)controls op operationeel niveau.
c) Testen van de (key) controls op strategisch, tactisch en operationeel niveau.
d) Evaluatie door het bestuur op de uitgevoerde controle d.m.v. de interne controle rapportage.
e) Opstellen door of namens het bestuur van 'in control' verklaring.

In het RAVC denkproces staan vier domeinen centraal, die in de figuur kort zijn toegelicht: kapitaalmanagement, producten en uitbesteding, reputatiemanagement en besturing.

De risicohouding van een bestuurslid is een bepaalde verhouding die het bestuurslid tussen beloning en risico wenst. Het gemiddelde van de onderscheiden risicohoudingen van de leden binnen het bestuur levert een algemene risicohouding van het fonds op. Het kennis hebben van de individuele risicohouding van de bestuursleden draagt bij aan de transparantie en diversiteit qua risicohouding aan de bestuurstafel.

De risicohouding en risicobereidheid wordt vastgesteld aan de hand van de vier domeinen van het RAVC©-model te weten:

Kapitaalmanagement | *Solvabiliteit, Liquiditeit & Rentabiliteit*

Het domein Kapitaalmanagement gaat vooral over:

- De beleggingsovertuigingen.
- Het (uitbestede) vermogensbeheer.
- Het Vereist Eigen Vermogen als kader voor risicobereidheid.
- De haalbaarheidstoets.

Product, Markt, Klant & (IT-)Organisatie | *Producten & (IT-)Processen*

Dit domein, kortweg 'Producten & Uitbesteding', gaat vooral over:

- De uitvoeringsprocessen.
- De pensioenregeling.
- De inrichting, monitoring, evaluatie en terugkoppeling ten aanzien van Service Level Agreements (SLA).
- De inrichting, de monitoring, de evaluatie en de terugkoppeling ten aanzien van de (IT-)organisatie en de uitbestedingsrelaties.
- De overtuigingen ten aanzien van de producten, de markt, de klanten en de (IT-)organisatie en de uitbestedingsrelaties.

Reputatiemanagement | *Imago, Identiteit & Integriteit*

Het domein Reputatiemanagement gaat vooral over:

- Imago (hoe zien anderen ons).
- Identiteit (wat wij willen uitstralen).
- Integriteit (handelen volgens onze kernwaarden).
- Compliance (volgens het principe 'comply or explain' voldoen aan wet- en regelgeving, waarbij onze kernwaarden leidend zijn).

Besturingsfilosofie | *Gedrag, Leiderschap & Cultuur*

Het domein Besturingsfilosofie gaat vooral over:

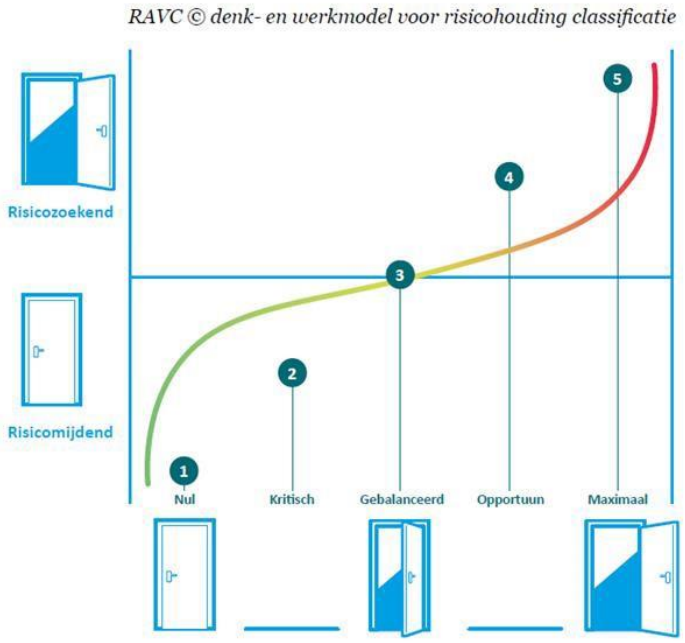
- Gedrag (hoe wij handelen).
- Leiderschap (onze regierol in de keten met uitbestedingsrelaties).
- Cultuur (bewustzijn, gericht op beheerste en integere bedrijfsvoering).
- Governance (inrichting van de organisatiestructuur, rollen en verantwoordelijkheden).
- Kernwaarden (waarden die leidend zijn in ons handelen).

Ten behoeve van het meetbaar maken van de bandbreedtes voor de risicobereidheid worden de risicobereidheidsprincipes verder geconcretiseerd door risicotolerantie. De risicotolerantie is uitgedrukt in criteria (risk appetite indicators) met grenzen uitgedrukt in een streefwaarde, 'ondermaats' en 'bovenmaats'.

Risicotolerantie – als toetssteen voor de (in volgende processtappen te bepalen) risico's en het risicobeheer – de verbinding tussen risicomanagement en performancemanagement. De toepassing van risicotolerantie wordt gerealiseerd door bandbreedtes te verankeren in beleid, afspraken met dienstverleners en de (risico-) management rapportages. Samen met de KPI's vormen zij de verbinding tussen risicomanagement en performancemanagement.

De risicotolerantiegrenzen zijn uitgedrukt in een minimum-, streef- en maximumwaarde. De streefwaarde duidt op een waarde die het bestuur, gezien de gekozen risicohouding, nastreeft. De ondergrens geeft aan welke waarde het bestuur, gezien de risicohouding ongewenst acht, en waarop dient te worden bijgestuurd. De maximumwaarde kan een indicatie zijn van het feit dat er te weinig risico wordt gelopen en/of te veel geïnvesteerd wordt in het beheersen van het risico.

B1.4 5-punts schaal risicohouding conform het RAVC© -model



Voor deze vier domeinen wordt op een 5-puntsschaal (classificatie) aangegeven wat de risicohouding (Risk Appetite) is:

- **Nul** (1): In dit geval is de risicohouding gekenmerkt door de wens dat er geen risico's worden genomen, vanuit de visie dat gewenste *rewards* niet vereisen dat een minimaal niveau van blootstelling aan risico's wordt geaccepteerd;
- **Kritisch** (2): Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's relatief laag te houden, vanuit de visie dat gewenste *rewards* vereisen dat een relatief laag niveau van blootstelling aan risico's wordt geaccepteerd;
- **Gebalanceerd** (3): Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's te balanceren, vanuit de visie dat gewenste *rewards* vereisen dat een gebalanceerd niveau van blootstelling aan risico's wordt geaccepteerd;
- **Opportuun** (4): Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's relatief hoog te houden, vanuit de visie dat gewenste *rewards* vereisen dat een relatief hoog niveau van blootstelling aan risico's wordt geaccepteerd;
- **Gemaximeerd** (5): In dit geval is de risicohouding gekenmerkt door de wens dat de blootstelling aan risico's maximaal is, vanuit de visie dat de gewenste *rewards* vereisen dat een maximale blootstelling aan risico's wordt geaccepteerd.

De risicohouding gaat niet over hoe het beleid op een bepaald moment *is*, maar hoe een bestuurder c.q. bestuur (per domein) een bepaalde verhouding tussen rewards en risico's *wenst*. De gekozen verhouding (nul; kritisch; gebalanceerd; opportunistisch; gemaximeerd) wordt per domein gemotiveerd.

B1.5 Heatmap

Heatmap

= bruto risico = netto risico

Impact / Kans	Zeer gering (1)	Laag (2)	Middel (3)	Hoog (4)	Catastrofaal (5)
Vrijwel zeker (5)					
Hoog (4)					
Middel (3)					
Laag (2)					
Zeer gering (1)					

Bijlage 2. Definities

Integraal risicomanagement:
Het interactieve proces van:
1. Het opstellen van de strategie en hieraan gekoppeld het risicoprofiel en de risicobereidheid;
2. Het identificeren van risico's;
3. Het opstellen en implementeren van het beleid voor risicobeheersing;
4. De uitvoering, monitoring en terugkoppeling over risico's en beheersmaatregelen.

Risicohouding:
De attitude van een persoon of groep van personen jegens een bepaalde onzekerheid of risico. Het gaat hier om het expliciteren van grondhouding ten aanzien van risico en rendement, volgens de classificatie Nul – Kritisch – Gebalanceerd – Opportuun – Maximaal. Deze schaal gaat geleidelijk van risicomijdend naar risico zoekend. Deze menskant van risicomanagement is fundamenteel voor besluitvorming- en besturingsprocessen.

Risicobereidheid:
Het vooraf (ex-ante) vaststellen van financiële en niet financiële strategische principes (*beliefs*) door het bestuur van waaruit het fonds zijn risicomanagementproces en risk governance inricht. Deze risicobereidheidsprincipes zijn de zogenaamde stoepranden van de organisatie. Het draagt bij aan de legitimatie van het fonds doordat het bestuur zijn principes (beliefs, financieel en niet financieel) transparant en expliciet uitdraagt en worden verankerd in beleid (normenkader).

Risicotolerantie:
Concretisering van risicobereidheidsprincipes, door normerende streefwaarden en grenzen te bepalen. Zogezegd de hoogte/dikte van stoepranden. Deze normeringen/ indicatoren zijn essentieel om concreet te toetsen of de uitvoering voldoet aan door het bestuur vastgestelde normering.

Risico:
Een gebeurtenis die het behalen van de (strategische) doelstellingen van het pensioenfonds kan belemmeren of blokkeren.

Beheersmaatregel:
Beheersmaatregelen zijn (organisatorische-, technische-, gedrags-) interventies die er toe leiden dat de geïdentificeerde risico's worden beheerst binnen het normenkader van het bestuur, zodat de doelstellingen behaald kunnen worden. Er moet ook een proces zijn waarmee wordt toegezien op de effectiviteit van beheersmaatregelen.
Soorten beheersmaatregelen:
- Preventief; bedoeld om het risico te voorkomen
- Detectief; bedoeld om het risico binnen acceptabele tijd te signaleren
- Repressief; bedoeld om schade als gevolg van het risico te beperken
- Correctief; bedoeld om door het risico geraakte bedrijfsproces(sen) binnen acceptabele tijd te herstellen