



**Pensioenfonds Achmea**

## **Integraal risicomanagement beleid**

[Versie september 2023]

## Versiebeheer

| Versie | Auteur           | Datum      | Omschrijving wijziging   |
|--------|------------------|------------|--|
| 0.8    | Vincent Straaten | 18-07-2019 | Revisie integraal risicomanagementbeleid   |
| 0.9    | Vincent Straaten | 11-09-2019 | Feedback Lenneke Roodenburg  |
| 1.0    | Vincent Straaten | 26-09-2019 | Feedback DB en CRM   |
| 1.1    | Vincent Straaten | 08-04-2021 | Met name herijking risicoraamwerk en proces risicobeoordeling en aanpassingen uit SIRA |
| 1.2    | Vincent Straaten | 05-09-2023 | Actualiseren tekst en bijlagen en feedback DB  |

## Inhoudsopgave

|  |    |
|--|----|
| Versiebeheer .....   | 2  |
| 1. Inleiding .....   | 4  |
| 1.1 Aanleiding .....   | 4  |
| 1.2 Leeswijzer: hoe is dit document opgebouwd? .....                                       | 4  |
| 2. Welke beleidskaders voor risicobeheersing hanteert het fonds? .....                     | 5  |
| 2.1 Beleidskader Solvabiliteitsbeheer .....  | 5  |
| 2.2 Beleidskader Management .....  | 6  |
| 2.3 Beleidskader Organisatie .....   | 7  |
| 3. Hoe dragen we zorg voor een beheerste bedrijfsvoering? .....                            | 8  |
| 3.1 Welke missie heeft ons fonds? .....  | 8  |
| 3.2 Wat is de visie en strategie van ons fonds? .....                                      | 8  |
| 3.3 Wat is randvoorwaardelijk voor IRM? .....  | 9  |
| 4. Hoe is de opzet IRM Governance? .....   | 11 |
| 4.1 Hoe is het 'three lines model' ingericht? .....  | 11 |
| 4.2 Wat zijn de uitgangspunten van de sleutelfuncties? .....                               | 12 |
| 5. Hoe is de uitvoering van de IRM Governance? .....                                       | 14 |
| 5.1 Wat zijn de taken en verantwoordelijkheden van de commissies en toezichtsorganen? .... | 14 |
| 5.2 Hoe zijn de sleutelhouderfuncties belegd? .....  | 15 |
| 6. Hoe is de invulling van het IRM raamwerk? .....   | 17 |
| 6.1 Welke processtappen doorloopt het fonds voor IRM? .....                                | 17 |
| 6.2 Hoe vindt risicobeheersing plaats? .....   | 18 |
| 7. Hoe vindt de eigenrisicobeoordeling plaats? .....                                       | 23 |
| 7.1 Wanneer wordt een eigenrisicobeoordeling uitgevoerd? .....                             | 23 |
| 7.2 Hoe vindt de praktische uitvoering van de ERB bij ons fonds plaats? .....              | 23 |
| 8. Inwerkingtreding .....  | 24 |
| Bijlage I: Hoofd- en subcategorieën risico's Pensioenfonds Achmea .....                    | 25 |
| Bijlage II: Beheersingskader .....   | 27 |
| Bijlage III: Scope van SIRA .....  | 29 |
| Bijlage IV: Begrippenlijst .....   | 30 |

# 1. Inleiding

## 1.1 Aanleiding

Het integrale risicomanagement beleid (IRM beleid) is geactualiseerd, omdat dit Volgens procedure minimaal eens in de 3 jaar moet plaatsvinden.

## 1.2 Leeswijzer: hoe is dit document opgebouwd?

In dit beleidsdocument wordt de opzet en uitvoering van het Integraal Risicomanagement (IRM) van Stichting Pensioenfonds Achmea (het fonds) beschreven.

De opbouw van het document is als volgt:

- In hoofdstuk 1: De inleiding
- In hoofdstuk 2. Welke beleidskaders voor risicobeheersing hanteert het fonds?
- In hoofdstuk 3. Hoe dragen we zorg voor een beheerste bedrijfsvoering?
- In hoofdstuk 4. Hoe is de opzet IRM Governance?
- In hoofdstuk 5. Hoe is de uitvoering van de IRM Governance?
- In hoofdstuk 6. Hoe is de invulling van het IRM raamwerk?
- In hoofdstuk 7. Hoe vindt de eigenrisicobeoordeling plaats?
- In hoofdstuk 8. Inwerkingtreding beleid

In de bijlagen zijn achtereenvolgens de risico hoofd- en subcategorieën, een rapportage-overzicht, scope systematische integriteitsrisicoanalyse (SIRA) en een begrippenlijst opgenomen.

## 2. Welke beleidskaders voor risicobeheersing hanteert het fonds?

Dit hoofdstuk beschrijft het kader waarbinnen het fonds de uit haar bedrijfsprocessen voortvloeiende risico's beheerst. Het fondsbestuur is en blijft verantwoordelijk voor de beleidsformulering en de uitvoering van het beleid, ook al is een deel van de werkzaamheden uitbesteed.

De IRM inrichting van ons fonds is gebaseerd op het risicomodel Financiële Instellingen Risico Methode (FIRM), als onderdeel van de toezichtaanpak FOCUS van De Nederlandsche Bank (DNB). Ons fonds hanteert in de basis dezelfde risicocategorieën, maar wijkt soms af om het fonds-specifiek te maken. Naast de gedefinieerde risicocategorieën van FIRM hanteert ons fonds ook de risico-overstijgende beheersingscategorieën: Management, Organisatie en Solvabiliteitsbeheer. Dit zijn beleidskaders die het fonds heeft ingericht en die overall mitigerend werken op alle risicocategorieën.

### 2.1 Beleidskader Solvabiliteitsbeheer

Solvabiliteitsbeheer richt zich op de financiële positie van ons fonds ten aanzien van strategisch beleid, financieel beleid en toeslagen- en premiebeleid. Ontwikkelingen van fluctuaties in renteniveau, dekkingsgraad en matching van verplichtingen en beleggingen vallen hier ook onder. De risicohouding is uitgangspunt voor het opstellen van het financieel beleid. Het fonds heeft dit als volgt ingevuld.

- 1 Vaststellen beleid:
  - Financieel beleid omvat beleggingsbeleid, verzekeringsbeleid, premiebeleid en toeslagenbeleid
  - Financieel beleid: gefundeerd op portefeuilleconstructie, ALM-studie en investment beliefs
  - Beleidsmatig vastgelegd in abtn en beleggingsplan
- 2 Implementatie beleid:
  - Uitwerking beleid in investmentcases, mandaten, overeenkomsten en richtlijnen
- 3 Monitoring beleid:
  - Periodieke evaluatie van beleid en beleidsuitwerkingen door:
    - o Uitvoering haalbaarheidstoets
    - o Periodieke beoordeling validiteit ALM-uitgangspunten
    - o Monitoring financiële positie en risico's aan de hand van diverse rapportages

## 2.2 Beleidskader Management

Onder management wordt een passende bestuursstructuur, bestuurlijke betrokkenheid, deskundigheid en aandacht voor integriteit verstaan. Dit beleidskader omvat verder aandacht voor strategie en de uitwerking daarvan. Een passende risico/control-houding en aandacht voor risicomangement is daarbij essentieel. Besturing en besluitvorming zijn gericht op het nemen van besluiten op de juiste bestuurlijke niveaus. Management is onder te verdelen naar:

- 1 Management kwaliteit en structuur:
  - Bestuursstructuur (paritair model) past bij de omvang en de verdere structuur van het fonds. Ons fonds heeft een bestuursbureau ingericht
  - Betrokkenheid van het bestuur en manager bestuursbureau (totaaloverzicht en weet wat speelt binnen ons pensioenfonds)
  - Bestuursleden en management beschikken over voldoende competenties, kennis en ervaring
  - Geschiktheidsplan inclusief opleidingsplan
  - Aandacht voor integriteit (o.a. belangenverstrengeling)
  - Er is sprake van een passend beloningsbeleid
  - Continuïteit, individuele kennis en kennis als geheel in bestuur
- 2 Strategie:
  - De missie en visie van het fonds leiden tot een strategie
  - Aanwezigheid van een visiedocument met een vastgelegde lange termijn strategie, uitgewerkt in concrete en haalbare doelstellingen en verwerkt in het jaarplan
  - De strategie is onafhankelijk van de sponsor vastgesteld
  - Inspelen op maatschappelijke thema's (bijvoorbeeld Maatschappelijk Verantwoord Beleggen)
  - Bekendheid met strategie binnen de totale fondsorganisatie
- 3 Risicohouding:
  - Risicomangement komt onafhankelijk van de uitvoeringsorganisatie tot oordelen
  - Identificatie van risico's en beperking van ongewenste risico's met beheersmaatregelen
  - Bereidheid van het bestuur tot het nemen van risico's en beheersmaatregelen
  - Bij het nemen van beleidsbeslissingen is sprake van afweging tussen rendement én risico binnen gestelde risicohouding
  - Risicoanalyse als expliciet onderdeel van het besluitvormingsproces
- 4 Besturing en besluitvorming:
  - Besluiten worden alleen genomen door een daartoe bevoegd orgaan
  - Het besluitvormingsproces is in overeenstemming met statutaire bepalingen, mandaatregelingen en overige fondsstukken
  - Schriftelijke mandatering fondsorganen en bestuursbureau
  - Schriftelijke vastlegging van besluiten (bijvoorbeeld in bestuursnotulen)
  - Openstaande acties worden bewaakt (bijvoorbeeld d.m.v. een actiepuntenlijst)

- Aanbevelingen van raad van toezicht (RvT) worden opgepakt
- Aanbevelingen van de internal auditor worden opgepakt
- Aanbevelingen van externe toezichthouders (o.a. van DNB, AFM, uit actuarieel en accountantsverslag) worden opgepakt
- Advies van verantwoordingsorgaan (VO) wordt meegenomen in besluitvorming
- Voldoende overleg tussen bestuur en management

### **2.3 Beleidskader Organisatie**

De wijze waarop de organisatie van het fonds is ingericht voor de uitvoering van de strategie en missie. Organisatie is onder te verdelen naar:

- 1 Organisatiestructuur:
  - De organisatiestructuur is eenduidig, duidelijk en stabiel
  - Een beschrijving van taken, bevoegdheden en verantwoordelijkheden (ook voor commissies)
  - Op gestructureerde en effectieve wijze uitvoeren van werkzaamheden
- 2 Managementinformatievoorziening:
  - Rapportagelijnen en inhoud sluiten aan op verantwoordelijkheidsstructuur
  - Het bestuur, intern en extern toezicht verkrijgen tijdig de gewenste informatie
  - Rapportages zijn inhoudelijk van voldoende niveau (zowel kwalitatief als kwantitatief)
- 3 Human Resources:
  - Adequate HR afspraken en beloningsbeleid (voor apparaat en bestuur)
  - Goede functieomschrijvingen
  - Voldoende bezetting in kwaliteit en kwantiteit
  - Aanwezigheid back-up voor spilfuncties
  - Interne samenwerking en communicatie
  - Aandacht voor interne communicatie en verbinding
- 4 Governance:
  - Kwaliteit uitvoerder internal audit (persoon en kantoor)
  - Governance en onafhankelijkheid volgens 3 lines model
  - Onafhankelijke compliance officer (andere dan bij de sponsor)
  - Scheidingadvies en assurance
  - Externe adviseurs kennen risico's binnen het fonds

## 3. Hoe dragen we zorg voor een beheerste bedrijfsvoering?

Pensioenfondsen moeten hun organisatie zó inrichten dat een beheerste bedrijfsvoering is gewaarborgd. Dat betekent dat ons pensioenfonds risico's, die bestaan bij de uitvoering van pensioenregelingen, in kaart brengt en maatregelen formuleert om deze risico's te beheersen. IRM is hiermee het middel om te zorgen dat de daadwerkelijke blootstelling aan risico's optimaal aansluit bij de gewenste mate van blootstelling. Deze wordt bepaald vanuit de missie, visie, strategie en doelstellingen van het fonds.

### 3.1 Welke missie heeft ons fonds?

Samen met onze deelnemers en cao-partijen zorgt Pensioenfonds Achmea met solide financieel beleid en goede en efficiënte uitvoering voor waardevast inkomen voor later. Onze missie is het effectief en efficiënt uitvoeren van de pensioenregeling voor de werkgevers en (voormalig) werknemers verbonden aan het Achmea-concern.

### 3.2 Wat is de visie en strategie van ons fonds?

Het bestuur ziet de komende jaren veel veranderingen voor de pensioensector. Dit betreft regelgeving (Wet toekomst pensioenen), toezicht en ontwikkelingen in uitvoering door onder andere meer digitalisering en individualisering. Daarnaast is er de impact en voortdurende onzekerheid van de financiële markten. Het fonds hanteert in deze voortdurend veranderende omgeving een consistent en prudent beleid, maar anticipeert tegelijkertijd en actief op de veranderingen, in samenwerking met uitvoerders en sociale partners.

Ons fonds is daarbij dé integrale uitvoerder voor pensioenregelingen van Achmea personeel en wil ook in de toekomst nieuwe pensioenregelingen blijven uitvoeren. We geloven in de kracht van het collectief: we delen verzekeringstechnische en beleggingsrisico's en we zorgen voor een (kosten)efficiënte uitvoering van de gewenste pensioenregelingen binnen één uitvoerder. De deelnemer kent één loket voor tweede pijler pensioenen en ontvangt heldere en éénvoudige informatie. Hiermee stellen we de deelnemer in staat om zelf de verantwoordelijkheid te nemen voor zijn/haar pensioeninkomen en zelf keuzes te kunnen maken binnen de mogelijke regelingen. Het fonds is het expertisecentrum pensioenen voor Achmea, werknemers en bonden. Als eigen ondernemingspensioenfonds met paritair ingericht bestuur staat het fonds dicht bij de deelnemers en de werkgever.



De visie en strategie van ons fonds zijn uitgewerkt in onderstaande strategische uitgangspunten:

1. Waardevast inkomen voor later: het fonds heeft een voldoende dekkinggraad en (verwacht)pensioenresultaat
2. Stakeholders zijn tevreden en vertrouwen het fonds
3. Het fonds heeft een efficiënt en houdbaar kostenniveau
4. Uitvoering en verantwoording is goed op orde en “in control”
5. Het fonds is compliant met wet- en regelgeving
6. Het fonds is klaar voor het nieuwe pensioencontract
7. Deelnemers zijn pensioenbewust en zelfredzaam
8. Het fonds draagt bij aan een duurzame samenleving

De strategische uitgangspunten zijn meetbaar gemaakt met key performance indicators (KPI's) en worden periodiek gemonitord.

### **3.3 Wat is randvoorwaardelijk voor IRM?**

Er zijn drie randvoorwaarden te onderkennen voor IRM. Die zijn in deze paragraaf nader uitgewerkt.

- **Integrale benadering**

Risico's doen zich voor binnen de verschillende lagen van de organisatie: vanaf het bestuur (bijvoorbeeld vaststellen beleid) tot en met vermogensbeheer en de pensioenadministratie bij de uitbestedingspartners. Een randvoorwaarde voor goed IRM is daarom een integrale benadering. Integraal betekent hierbij:

- Geïntegreerd in de dagelijkse uitvoering- en besluitvormingsprocessen van het Fonds
- Met betrekking tot de verschillende lagen van de organisatie
- Met het overzicht over het geheel van de risico's
- Rekening houdend met de onderlinge samenhang van (sommige) risico's

- **Compliance**

Op grond van de Pensioenwet, het Besluit FTK en het Besluit uitvoering Pensioenwet moet een pensioenfonds onder meer beschikken over een werkzaam risicomanagementsysteem (risicostrategieën, -processen en -rapportageprocedures). Een pensioenfonds is op grond hiervan bijvoorbeeld verplicht om zorg te dragen voor een systematische analyse van de risico's. Zie bijlage III voor de scope van integriteitsrisico's in de SIRA.

In wet- en regelgeving zijn verschillende eisen opgenomen waaraan het risicomanagement moet voldoen. Compliant zijn aan wet- en regelgeving op het gebied van risicomanagement is daarmee ook een belangrijke randvoorwaarde waaraan IRM moet voldoen.

- **Cultuur**

Een cultuur, waarin sprake is van risicobewustzijn is randvoorwaardelijk voor IRM. Dit gaat om risicobewustzijn bij de fondsorganen en bestuursbureau. Het expliciet maken van de risicohouding en periodiek bespreken van de resultaten van de meting van risico's draagt daar bijvoorbeeld in sterke mate aan bij. Maar ook risicobewustzijn bij de uitvoering. Bijvoorbeeld door risico's, controles en de rapportages hierover een vast onderdeel te laten zijn van de afspraken die gelden bij de uitvoering.

Het risicomanagement kan pas succesvol zijn als de gehele organisatie met bestuur, RvT, VO, bestuursbureau, adviseurs en uitbestedingspartners verantwoordelijkheid neemt voor het beheersen van risico's.

## 4. Hoe is de opzet IRM Governance?

### 4.1 Hoe is het 'three lines model' ingericht?

De basis voor het inrichten van het IRM van ons fonds is een heldere en zuivere verdeling van taken, verantwoordelijkheden en bevoegdheden. Op basis van het principe van 'three lines model' is onderscheid gemaakt naar risico-eigenaren (1e lijn), controlefunctie (2e lijn) en interne audit (3e lijn). In onderstaande schematische weergave is het three lines model nader uitgewerkt voor ons fonds.

| Bestuur   |  |  |   |
|---|--|--|---|
| Eerste lijn   | Tweede lijn  | Derde lijn   | Overig  |
| DB, en<br>Commissies CP en<br>CBM   | Commissie CRM (*)                                      | Internal audit<br>EY                                     | Accountant PWC<br>certificerend<br>actuaris WTW |
| Uitbestedingspartijen<br>en adviseurs<br>- Achmea PS<br>- Administratie<br>- Juridisch<br>- Communicatie<br>- Actuarieel<br>- Advies<br>- Achmea IM<br>- Caceis<br>- Almazara<br>-<br>- | Uitbestedingspartijen<br>en adviseurs:<br>R&C functies | Uitbestedingspartijen<br>en adviseurs:<br>internal audit | Beleggingsadvies<br>Triple A                    |

\* Inclusief compliance officer, privacy officer en voor tweede lijn ingehuurd adviseurs

*Figuur 1: three lines model Pensioenfonds Achmea*

- **Risico-eigenaar**

Een risico-eigenaar (eerste lijn) is een rol of een individu die verantwoordelijk is voor een bepaald risico en de rapportage hierover. Het risico-eigenaarschap, waaronder monitoring van de werking van relevante beheersmaatregelen, is belegd in de diverse

commissies. Zie hoofdstuk 5 voor een nadere toelichting op de commissies. De risico-eigenaar is verantwoordelijk voor het beheren en beheersen van alle aspecten van het risico. Dit vindt plaats door:

- Het inventariseren van de relevante risico's
- Het vaststellen van de scenario's en beheersmaatregelen
- De beheersmaatregelen leiden tot keycontrols, die periodiek worden uitgevoerd. De effectieve werking dient te worden aangetoond met een toelichting en (verwijzing naar) de vereiste evidence

- **Controlefunctie**

Een controlefunctie (een tweede lijn) beoordeelt, monitort, rapporteert en heeft een adviserende en initiërende rol met betrekking tot risico's en het risicobeheer. Deze verantwoordelijkheid is gescheiden van de verantwoordelijkheid van de risico-eigenaar. De controlefunctie wordt ingevuld door de risicobeheerfunctie, de compliance officer, de privacy officer en de actuariële functie (zoals beschreven in het vervolg van dit hoofdstuk) die de 2e lijn vormen.

- **Interne auditfunctie**

De interne auditfunctie (een derde lijn) beoordeelt periodiek de adequaatheid en doeltreffendheid van de interne controle. De auditfunctie legt primair verantwoording af aan het bestuur. Deze functie wordt ingevuld door de sleutelfunctiehouder en -vervuller Interne Audit en vormt de 3e lijn.

## 4.2 Wat zijn de uitgangspunten van de sleutelfuncties?

- **IORPII**

Op grond van artikel 143a Pensioenwet, dat in werking is getreden met ingang van 1 januari 2019 ter implementatie van de IORP-II Richtlijn, dient een pensioenfonds te beschikken over een risicobeheerfunctie, interne auditfunctie en actuariële functie.

- **Risicobeheerfunctie**

De risicobeheerfunctie beoordeelt, monitort en rapporteert over het risicobeheersysteem. Ook heeft de risicobeheerfunctie een initiërende en adviserende rol bij het vormgeven van het risicobeheer.

- **Interne auditfunctie**

De interne auditfunctie is belast met het uitvoeren van (interne) audits binnen de bedrijfsvoering van een pensioenfonds.

- **Actuariële functie**

De actuariële functie ziet onder meer toe op de berekeningen van de technische voorzieningen en premiestelling van het pensioenfonds.

- **Uitgangspunten sleutelfuncties**

Het bestuur is verantwoordelijk voor de inrichting van deze functies op een wijze die voldoet aan de vereisten zoals geformuleerd in de wet- en regelgeving. Daarbij mag het bestuur rekening houden met de omvang, de aard en de schaal en de complexiteit van de werkzaamheden van het fonds.

Bij de invulling van de sleutelfuncties is een aantal uitgangspunten van toepassing.

- **Proportionaliteit**

Pensioenfonds Achmea is een middelgroot fonds. Bij de inrichting van de sleutelfuncties is rekening gehouden met de omvang en interne organisatie van het fonds, alsmede met de omvang, de aard, de schaal en de complexiteit van de werkzaamheden.

Er zijn hiermee verschillende mogelijkheden om binnen de wettelijke voorwaarden te voldoen aan de vereisten omtrent de sleutelfuncties. Het bestuur is verantwoordelijk voor het naar behoren inrichten van de sleutelfuncties. De toezichthouder DNB ziet hierop toe.

- **Sleutelfunctiehouder versus sleutelfunctievervuller**

Bij het inrichten van de sleutelfuncties wordt onderscheid gemaakt tussen personen die sleutelfuncties vervullen en houders van een sleutelfunctie. De sleutelfunctiehouder is één persoon en eindverantwoordelijk voor de uitoefening van de taken die vallen onder de sleutelfunctie. Daarnaast kunnen overige personen betrokken zijn bij het vervullen van een sleutelfunctie.

- **Geschikt en betrouwbaar**

Het bestuur is verantwoordelijk voor het toetsen van de geschiktheid en betrouwbaarheid van de personen die betrokken zijn bij het vervullen van een sleutelfunctie. DNB kan, indien zij daartoe aanleiding ziet, de personen onderwerpen aan een toets.

## 5. Hoe is de uitvoering van de IRM Governance?

Zoals in het voorgaande hoofdstuk is beschreven betreft de IRM Governance een juiste scheiding van taken, bevoegdheden en verantwoordelijkheden. De hierbij behorende uitvoering wordt in dit hoofdstuk nader beschreven aan de hand van de ingestelde commissies en de sleutelfuncties.

### 5.1 Wat zijn de taken en verantwoordelijkheden van de commissies en toezichtsorganen?

Ons fonds heeft een IRM model ingesteld. Het bestuur is eindverantwoordelijk voor het IRM en zorgt voor een passende beheersing van alle risico's waar het fonds mee wordt geconfronteerd. Vanuit die verantwoordelijkheid draagt het bestuur zorg voor de inrichting van de governance, waaronder verdeling van de risico-eigenaren en sleutelfuncties. Door middel van mandaatregelingen is de uitvoering en het risico-eigenaarschap gedelegeerd naar de commissies. Deze paragraaf beschrijft het dagelijks bestuur, de drie ingestelde commissies en hun mandaat vanuit risicoperspectief.

- **Het dagelijks bestuur**

Het dagelijks bestuur (DB) is verantwoordelijk voor het initiëren van het door het bestuur vast te stellen integraal risicobeleid. Het DB is risico-eigenaar van de volgende risicogebieden: de beheersingscategorieën management en organisatie, het strategisch- en omgevingsrisico, het integriteitsrisico, het operationeel risico, het juridische en IT-risico. De 3 laatste risico's hebben betrekking op de interne organisatie van pensioenfonds Achmea.

- **Commissie balansmanagement**

De commissie balansmanagement (CBM) is verantwoordelijk voor het balansmanagement inclusief financieel beheer bij het fonds. Deze verantwoordelijkheid valt uiteen in twee hoofdonderwerpen: beleidsvoorbereiding en uitvoering. De CBM is verantwoordelijk voor de beheersingscategorie solvabiliteitsbeheer en de volgende risicogebieden: het matching/renterisico, het valutarisico, het marktrisico, het kredietrisico, het ESG en klimaatrisico, het uitbestedingsrisico, het integriteitsrisico, het juridische en IT-risico m.b.t. fiduciair- en vermogensbeheer en onderpandbeheer.

- **Commissie pensioenen**

De verantwoordelijkheid van de commissie pensioenen (CP) bevat net als bij de CBM beleidsvoorbereiding en -uitvoering. De CP is verantwoordelijk voor de volgende risicogebieden: het integriteitsrisico, het verzekeringstechnische risico, het uitbestedingsrisico, het operationeel risico, het juridische en het IT-risico m.b.t. pensioenbeheer en communicatie.

- **Commissie risicomanagement**

De commissie risicomanagement (CRM) adviseert, ondersteunt en monitort de overige bestuurscommissies (CBM, CP) en het dagelijks bestuur op het gebied van risicomanagement. Hiermee borgt de CRM het integraal risicomanagement (inclusief risicobeheersing- en controlesystemen) van de tweede lijn.

De commissie zorgt voor een effectieve challenge van de belangrijke risico's die het fonds bij de beleidsontwikkeling of –uitvoering loopt. Voor onderwerpen met een hoog risicokarakter zorgt de commissie voor een eigen risicobeoordeling of opinie ten aanzien van het onderwerp.

- **Raad van toezicht**

De raad van toezicht (RvT) is onder meer belast met het toezien op adequate risicobeheersing door het bestuur. Om de RvT in staat te stellen toe te zien op een adequate risicobeheersing wordt de RvT periodiek geïnformeerd over het IRM-beleid en de uitvoering daarvan.

- **Verantwoordingsorgaan**

Het verantwoordingsorgaan (VO) beoordeelt onder meer of het bestuur rekening houdt met de diverse belanghebbenden. Daarbij kijkt het orgaan naar hoe het bestuur handelt en welke beleidskeuzes het maakt. Via het VO zijn deelnemers en pensioengerechtigden ook nauw betrokken bij de uitvoering van de pensioenregeling. Het VO adviseert het fonds over diverse aangelegenheden.

De dagelijkse uitvoering is belegd binnen het bestuursbureau. Het DB, de drie commissies, RvT en VO zijn geen uitvoerende organen, maar hebben een coördinerende en vertegenwoordigende rol.

## **5.2 Hoe zijn de sleutelhouderfuncties belegd?**

Op het fonds zijn drie sleutelhouderfuncties van toepassing. Het betreft de sleutelfuncties Risicobeheer, Actuariel en Interne Audit. De inrichting van de drie sleutelfuncties bij het fonds is gebaseerd op het principe van het 'three lines model' zoals beschreven in paragraaf 2.1. De risicobeheerfunctie en actuariële functie zijn beide onderdeel van de controlefunctie (2e lijn). De interne auditfunctie vormt de 3e lijn.

- **Risicobeheer**

De sleutelfunctiehouder Risicobeheer is de voorzitter van de commissie Risicomanagement. De sleutelfunctie vervuller is de risicomanager van het fonds. Beide functies zijn hiermee intern belegd.

De onafhankelijkheid van de sleutelfunctiehouder en -vervuller is geborgd in de separate 2e lijns positie van de commissie Risicomanagement, waarbinnen de functie is belegd. De sleutelfunctiehouder is tevens geen lid van een andere commissie binnen het fonds. Er is sprake van scheiding tussen 1e lijns uitvoering (overig bestuur) en 2e lijns risicobeoordeling en advisering (commissie Risicomanagement).

- **Actuarieel**

De sleutelfunctiehouder en -vervuller Actuarieel is belegd bij de certificerend actuaris.

- **Interne Audit**

De sleutelfunctiehouder Interne Audit is intern belegd bij de secretaris van het DB. Het DB heeft geen verantwoordelijkheid voor de eerstelijns activiteiten pensioenbeheer, vermogens- en fiduciair beheer. De sleutelfunctie vervuller is extern belegd bij een advieskantoor voor de borging van de onafhankelijkheid. De onafhankelijkheid van de 3<sup>e</sup> lijns beoordeling is hiermee voldoende geborgd.

Voor zowel risicobeheer, actuarieel en interne audit geldt dat de sleutelfunctiehouder de informatie en rapportage ontvangt vanuit de 1e lijn. Daarnaast is de onafhankelijkheid gewaarborgd in de rechtstreekste toegang tot, en functionele rapportage aan de RvT.



## 6. Hoe is de invulling van het IRM raamwerk?

### 6.1 Welke processtappen doorloopt het fonds voor IRM?

Onderdeel van de in hoofdstuk 2 genoemde eindverantwoordelijkheid van het bestuur betreft de inrichting van een IRM-raamwerk. De missie, visie en strategie zijn tezamen met de inrichting IRM opgenomen in dit integraal risicomanagementbeleidsplan.

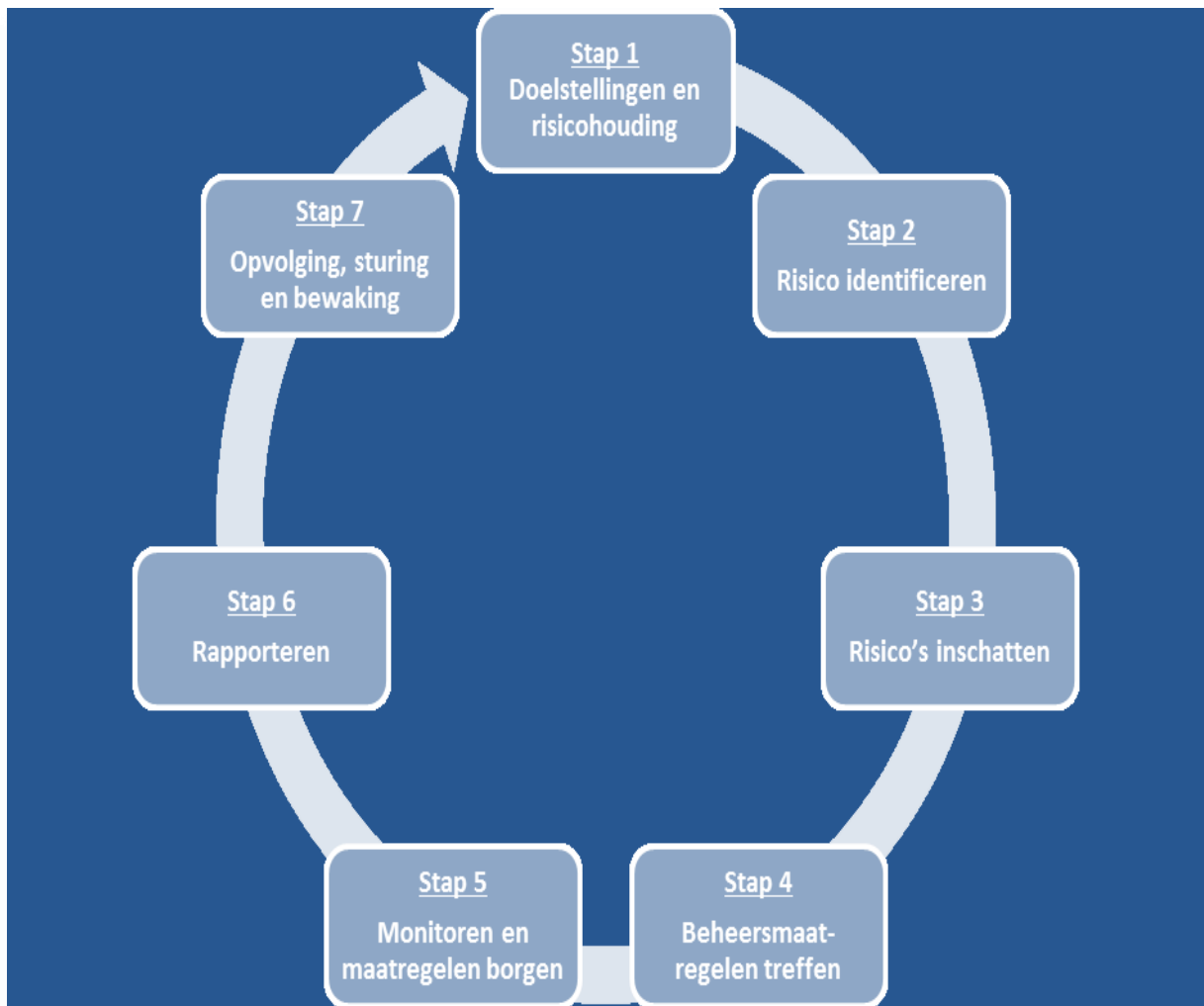
**De geïdentificeerde strategische risico's zijn meetbaar gemaakt aan de hand van KPI's en opgenomen in het jaarplan IRM.**

Een overzicht van alle geïdentificeerde risico's, scenario's en beheersmaatregelen is opgenomen in een overzicht van het risicoraamwerk.

De risicomanagementcyclus verloopt volgens de onderstaande stappen (schematisch weergegeven in figuur 1):

1. Doelstellingen en risicohouding: wat zijn de doelstellingen en welke blootstelling is wenselijk en acceptabel?
2. Identificatie: met welke risico's wordt het pensioenfonds geconfronteerd en welke scenario's zijn van toepassing?
3. Risico's inschatten: hoe groot worden deze risico's ingeschat?
4. Beheersmaatregelen treffen: formulering van gewenste beheersingsniveau, past het risico binnen de risicohouding en welke acties zijn wenselijk?
5. Monitoren en maatregelen borgen: Worden de beheersmaatregelen uitgevoerd en vindt hier onafhankelijke toetsing op plaats?
6. Rapporteren: Wordt de effectiviteit van de beheersmaatregelen periodiek gerapporteerd?
7. Opvolgen, sturen en bewaken: Vindt continue verbetering van het IRM plaats?

Op de volgende pagina is een schematische weergave van de risicomanagementcyclus, zoals deze binnen het fonds wordt gehanteerd.



*Figuur 2: Risicomanagementcyclus*

## 6.2 Hoe vindt risicobeheersing plaats?

### ***Doelstellingen en risicohouding financiële risico's: welke blootstelling is wenselijk en acceptabel?***

Het fonds heeft strategische uitgangspunten (doelstellingen) geformuleerd en vervolgens een risicohouding bepaald ten aanzien van de risico's die deze uitgangspunten kunnen bedreigen.

Het fonds is een financiële instelling. Het bewust aangaan en beheersen van financiële risico's behoort daarom tot de kerntaken van het fonds en houdt rechtstreeks verband met de missie van het fonds om met solide financieel beleid zorg te dragen voor een waardevast inkomen voor later.

De financiële risicohouding is door het fondsbestuur vastgesteld voor de korte en lange termijn. Deze risicohouding (lange en korte termijn) is nader uitgewerkt in de abtn. Het

fondsbestuur ziet de komende jaren veel veranderingen voor de pensioensector. Dit betreft regelgeving (zoals de Wtp), toezicht en ontwikkelingen in uitvoering door onder andere meer digitalisering en individualisering.

De risicohouding voor de niet-financiële risico's is conform onze missie het effectief en efficiënt uitvoeren van de pensioenregeling voor de werkgevers verbonden aan het Achmea-concern. Om een kostenefficiënte organisatie te bewerkstelligen kan het fonds besluiten om werkzaamheden uit te besteden, mits de hiermee gepaard gaande risico's en kosten beheersbaar blijven.

***Risico-identificatie: met welke risico's wordt het fonds geconfronteerd?***

Het fonds heeft op basis van een risicoanalyse uit het totaal aantal risico's een top 5 samengesteld van strategische risico's, waarop extra focus wordt betracht. Drie van deze risico's zijn financieel van aard. Deze risico's zijn nader uitgewerkt in het IRM jaarplan.

***Risico's inschatten: hoe groot worden deze risico's ingeschat?***

Risico's worden bruto (zonder beheersmaatregelen) en netto (met beheersmaatregelen) ingeschat en op zowel kans alsook impact is een individuele tolerantie vastgesteld. Het fonds maakt bij de analyse gebruik van een kans en impact inschatting op een schaal van 1 tot en met 4. Deze schaalverdeling wordt enerzijds groot genoeg geacht om voldoende onderscheid te maken tussen de risico's en wordt anderzijds klein genoeg geacht om 'schijnnaauwkeurigheid' en inconsistentie in de risicoanalyse te vermijden. Voor financiële risico's is onderstaande impact definitie van toepassing.

|             | Kans  | Impact  |
|-------------|---|---|
| Laag        | Onwaarschijnlijk dat het zich voordoet de komende 5 jaar, of heeft zich niet eerder voorgedaan binnen Pensioenfonds Achmea. | Dekkingsgraad wordt niet negatief beïnvloed   |
| Beperkt     | Doet zich mogelijk voor binnen 3 jaar, of heeft zich voorgedaan de afgelopen 5 jaar   | Dekkingsgraad daalt met maximaal 5%, of dekkingsgraad daalt onder 110% (uitgaande van een financieel solide positie van Pensioenfonds Achmea).    |
| Aanzienlijk | Heeft de potentie om op te treden binnen het komend jaar, of heeft zich voorgedaan de afgelopen 2 jaar.                     | Dekkingsgraad daalt met maximaal 10%, of dekkingsgraad daalt onder 105%.% (uitgaande van een financieel solide positie van Pensioenfonds Achmea). |
| Hoog        | Treedt het komend jaar op, of heeft zich het afgelopen jaar voorgedaan  | Dekkingsgraad daalt met meer dan 10%, of dekkingsgraad daalt onder 100% (uitgaande van een financieel solide positie van Pensioenfonds Achmea)    |

Tabel 1: Kans / impact financiële risico's

Voor niet-financiële risico's is onderstaande impact definitie van toepassing.

|             | Kans  | Impact  |
|-------------|---|---|
| Laag        | Onwaarschijnlijk dat het zich voordoet de komende 5 jaar, of heeft zich niet eerder voorgedaan binnen het Pensioenfonds Achmea. | Risico op interne negatieve / kritische berichtgeving (incl. uitvoerders).<br>Het niveau van dienstverlening van Pensioenfonds Achmea wordt beïnvloed, maar geen gevolgen voor de tevredenheid van deelnemers.<br>Makkelijk te herstellen.  |
| Beperkt     | Doet zich mogelijk voor binnen 3 jaar, of heeft zich voorgedaan de afgelopen 5 jaar   | Risico op interne negatieve / kritische berichtgeving (incl. uitvoerders).<br>Het niveau van dienstverlening van Pensioenfonds Achmea wordt beïnvloed, met als gevolg een beperkte daling van de tevredenheid van deelnemers.<br>Is te herstellen.  |
| Aanzienlijk | Heeft de potentie om op te treden binnen het komend jaar, of heeft zich voorgedaan de afgelopen 2 jaar.                         | Risico op negatieve publiciteit richting pensioensector.<br>Negatieve reacties vanuit DNB/AFM.<br>Het niveau van dienstverlening van Pensioenfonds Achmea wordt beïnvloed, met als gevolg een behoorlijke daling van de tevredenheid van deelnemers.<br>Is moeilijk te herstellen.        |
| Hoog        | Treedt op het komend jaar, of heeft zich het afgelopen jaar voorgedaan.   | Risico op negatieve publiciteit richting pensioensector.<br>Structureel negatieve reacties vanuit DNB/AFM.<br>Het niveau van dienstverlening van Pensioenfonds Achmea wordt beïnvloed, met als gevolg een grote daling van de tevredenheid van deelnemers.<br>Erg moeilijk te herstellen. |

Tabel 2: kans / impact niet-financiële risico's

### **Beheersmaatregelen treffen: risicobeoordeling en risicobehandeling**

Voor alle risico's zijn scenario's opgesteld en op basis van deze scenario's worden beheersmaatregelen geformuleerd. Op ieder scenario is minimaal één beheersmaatregel van toepassing. Een beheersmaatregel is niet automatisch ook een keycontrol. De toetsing van een keycontrol wordt in tegenstelling tot een beheersmaatregel periodiek vastgelegd in de hiervoor ingerichte vastleggingstool inclusief score (effectief / niet-effectief) toelichting en evidence.

***Monitoren en maatregelen borgen: Worden de beheersmaatregelen uitgevoerd en vindt hier onafhankelijke toetsing op plaats?***

De keycontrol beschrijvingen zijn duidelijk door het gebruik van de 4W's (wie, wat, wanneer en waarmee). Periodiek worden de KPI's en keycontrols uitgevoerd door de 1e lijn aan de hand van een toelichting, vaststelling effectiviteit en (verwijzing naar) evidence. De risicomanager toetst de vastlegging op juistheid, tijdigheid en volledigheid.

***Rapporteren: Wordt de effectiviteit van de beheersmaatregelen periodiek gerapporteerd?***

De commissies en het DB stellen per kwartaal een risico- en verantwoordingsrapportage op, waarin de aan hen toebedeelde risico's en KPI's worden toegelicht met onder meer de bevindingen op de uitgevoerde en keycontrols.

***Opvolgen, sturen en bewaken: vindt continue verbetering van het IRM plaats?***

Het volledig doorlopen van de IRM-cyclus waarborgt dat er periodiek een evaluatie, en als onderdeel daarvan aanvullende risico-identificatie, plaatsvindt waaruit aanvullende risico's of risicocategorieën kunnen worden benoemd. Daarom vindt bij ons fonds jaarlijks een evaluatie van de werking van het IRM plaats. Dit gebeurt aan de hand van een herijking, waarbij de 1e lijn in samenwerking met de risicomanager de risico's, scenario's beheersmaatregelen en keycontrols kritisch evalueert en aanpast waar benodigd. Daarnaast vindt bij tussentijdse wijzigingen in het risicoprofiel per kwartaal een evaluatie en aanpassing plaats. De evaluatie kan worden gezien als de laatste stap van een herhalend proces.

De evaluatie van de KPI's en strategische top risico's vindt tegelijk met de eigenrisicobeoordeling plaats: eens in de drie jaar en tussentijds bij zogenoemde trigger events. Het bestuur beoordeelt dan in hoeverre de benoemde doelstellingen respectievelijk risico's nog steeds de KPI's en strategische top risico's vertegenwoordigen (zie ook hoofdstuk 7).

In afstemming met de commissies en DB stelt CRM daarnaast (gevraagd en ongevraagd) een risicoparagraaf of risico notitie op bij onderwerpen van de commissies en het DB die een tweede lijn beoordeling behoeven. Dit betreft:

1. Nieuw beleid en inhoudelijke beleidsaanpassingen
2. Voorstellen met aanzienlijke en hoge impact op de kritische risicobeheersing (risicoraamwerk) of onze kritische prestatie indicatoren. Zie bijlage II voor een nadere toelichting op kans en impact.
3. Selectievoorstellen- en besluiten beleggingen

De risicobeoordelingen op punten 1 en 2 worden behandeld in het bestuur en vervolgens teruggekoppeld naar commissies en DB. Dit proces verloopt als volgt:

- (concept) Risicobeoordeling wordt opgesteld in een aparte notitie indien het selectievoorstellen- en besluiten beleggingen betreft

- Bij overige risicobeoordelingen bestaat naast een aparte notitie ook de mogelijkheid om de risicobeoordeling op te nemen in een risicoparagraaf in de door de 1e lijn opgestelde voorlegger over het desbetreffende onderwerp
- Incidenteel kan bij verlaat ingebrachte eerste lijn onderwerpen, waar een risicobeoordeling benodigd is, worden volstaan met een mondelinge toelichting van de sleutelfunctiehouder risicobeheer in de bestuursvergadering

Selectievoorstellen (punt 3) gaan niet langs het bestuur en de risicobeoordelingen hierop worden op de eerstvolgende vergadering van CBM geagendeerd.

De risicobeoordeling wordt met standaardindeling opgesteld:

- Proces (conform procedure en in lijn met beleid / beleidskaders)
- Risicoprofiel (juiste risico's ingeschat en in lijn met risicobereidheid)
- Tweedelijns oordeel

Terugkoppeling: de notitie wordt voorbereid door CRM

- Eventuele aanpassingen voortkomend uit de CRM worden doorgevoerd in de risicobeoordeling en teruggekoppeld naar 1e lijn met CRM ter informatie in CC.
- Aanbevelingen uit de risicobeoordeling dienen altijd te zijn afgestemd met én geaccepteerd door de (gedelegeerd) verantwoordelijke(n)
- Rapportage: definitieve risicobeoordeling notities komen op de agenda van de eerstvolgende bestuursvergadering
- Specifiek bij selectievoorstellen- en besluiten voor beleggingen wordt de definitieve risicobeoordeling notitie via Memo lopende zaken van de CBM gerapporteerd naar die commissie

CRM monitort auditissues en aanbevelingen (geaccepteerde verbeteracties) uit de risicobeoordelingen. CRM heeft bij onenigheid van standpunten altijd de mogelijkheid om te escaleren naar het bestuur.

- Monitoring: auditissues en verbeteracties (geaccepteerde aanbevelingen) worden door de risicomanager vastgelegd in de module 'issuemanagement' in Cothesys met eigenaar, classificatie en einddatum
- De verbeteracties worden opgenomen in de actielijst van de commissie en DB. De voortgang wordt zo gemonitord door commissies en DB

## 7. Hoe vindt de eigenrisicobeoordeling plaats?

### 7.1 Wanneer wordt een eigenrisicobeoordeling uitgevoerd?

Voor de inrichting van het risicobeheer en de onderbouwing van strategische besluitvorming is de eigenrisicobeoordeling (ERB) van essentieel belang. De ERB maakt integraal onderdeel uit van de strategie en het risicobeheer van de instelling. Het fonds voert tenminste driejaarlijks een reguliere eigenrisicobeoordeling (ERB) uit. Deze frequentie is geënt op de (strategische) beleidscyclus van het fonds, zodat de ERB een onderbouwing is voor strategische beleidsbesluiten. Daarnaast zijn er twee soorten omstandigheden die om een tussentijdse actualisatie van (een deel van) de ERB vragen:

1. Significante wijziging in het risicoprofiel (bijvoorbeeld een significante wijziging in de risicohouding). Indien de significante wijziging enkel een specifieke pensioenregeling betreft, zal de tussentijdse ERB beperkt blijven tot die pensioenregeling
2. Strategisch besluit met een materiële impact op het risicoprofiel. Voorafgaand aan een strategisch besluit is het noodzakelijk om al zicht te hebben op de impact ervan op het risicoprofiel, de benodigde beheersmaatregelen en de bestaande ERB. Een voorbeeld hiervan is een besluit tot de sluiting van een fonds

Een gedeeltelijke actualisatie van de ERB kan toereikend zijn indien de impact van een besluit beperkt blijft tot een onderdeel van de ERB.

De beleidsmatige verankering van de ERB door het fonds betreft allereerst de incorporatie van de ERB in het risicobeheer van de instelling en de wijze waarop de risicobeheercyclus wordt doorlopen. Het fonds dient alle risico's te identificeren, beleid op te stellen voor de risicobeheersing en terugkoppeling te geven over risico's en beheersmaatregelen. De toevoeging van de ERB geeft het fonds inzicht in de materiële risico's en de mogelijke consequenties hiervan voor de financiële positie van het fonds en de pensioenen van deelnemers. Het fonds beoordeelt daarmee periodiek de effectiviteit en de doelmatigheid van het risicobeheer.

De ERB zal worden uitgevoerd en vastgesteld aan de hand van het IRM raamwerk van het fonds. Bij deze ERB zal de doelmatigheid van het integrale risicomanagement framework en daarbinnen het risicomanagementbeleid worden geëvalueerd.

### 7.2 Hoe vindt de praktische uitvoering van de ERB bij ons fonds plaats?

De ERB is bedoeld om inzicht te krijgen in de samenhang tussen de strategie van het fonds en de strategische en materiële risico's. De ERB bestaat enerzijds uit een statisch deel met de beschrijving van en verwijzing naar het ERB proces, IRM proces en de governance. De ERB bestaat anderzijds uit een dynamisch deel met een actueel risicoprofiel en scenario's.

De ERB wordt bij ons fonds minimaal driejaarlijks uitgevoerd, maar indien zich een trigger event voordoet ten aanzien van de strategische Top 5 risico's dan vindt tussentijds een (gedeeltelijke) ERB plaats op dat specifieke risico met bijbehorende scenario('s). De strategische Top 5 risico's zijn opgenomen in het IRM jaarplan, dat jaarlijks wordt geëvalueerd.

De keuze van de scenario's dient aan te sluiten bij de trigger en de belangrijkste risico's. Scenario-analyse zal worden ingezet voor het inzichtelijk maken van de financiële en niet-financiële risico's. Belangrijke uitgangspunten voor deze scenario's zijn:

1. Zwaar, maar reëel
2. Specifiek voor ons fonds
3. Bevat materiële risico's
4. Relevant voor deelnemers

Het formuleren van een centrale vraag helpt bij het aanbrengen van focus in de uitvoering van de ERB. Recentelijk is naar aanleiding van actuele triggers (o.a. pensioenakkoord) door ons fonds een gedeeltelijke ERB uitgevoerd op het omgevingsrisico. Onderstaande centrale vragen zijn nader uitgewerkt in deelvragen ('wat als'):

1. Wat zijn de mogelijke gevolgen van een veranderende omgeving (maatschappelijke en economische ontwikkelingen) voor ons fonds?
2. Wat zijn de mogelijke gevolgen van het pensioenakkoord voor ons fonds?

Vervolgens is de impact ervan uitgewerkt in een SWOT analyse, die de basis vormt voor de beoordeling van de effectiviteit en doelmatigheid van het risicobeheer en beheersingskader (zie bijlage II) van ons fonds.

De uitkomsten van de ERB worden vastgelegd in een eindrapportage ERB die, na vaststelling door het bestuur, wordt gedeeld met DNB.

## 8. Inwerkingtreding

Het IRM beleid is in de bestuursvergadering van 21 september 2023 voor het laatst vastgesteld. Het gewijzigde beleid treedt per die datum in werking. Het laatst gewijzigd beleid is het geldende beleid.



## Bijlage I: Hoofd- en subcategorieën risico's Pensioenfonds Achmea

In deze bijlage is een overzicht opgenomen van alle hoofd en subcategorie risico's (financieel en niet-financieel) die het fonds heeft geïdentificeerd. Het totale overzicht van risico's, scenario's, beheersmaatregelen en keycontrols is opgenomen in het excelbestand 'Totaaloverzicht risico en beheersmaatregelen'. De risicocategorieën uit het risicoraamwerk sluiten aan op de in IORP II benoemde thema's'

### Financiële risico's

- 1 Matching-/renterisico
  - Rente
  - Liquiditeit
- 2 Marktrisico
  - Prijsvolatiliteit
  - Marktliquiditeit
  - Concentratie en correlatie
  - Valuta
- 3 Kredietrisico
  - Vastrentende waarden
  - Derivaten
- 4 ESG en klimaatrisico
- 5 Verzekeringstechnisch risico

**Niet financiële risico's**

## 6 Omgevingsrisico

- Concurrentie en afhankelijkheid
- Reputatie

## 7 Operationeel risico

- Kosten
- Personeel / bestuur
- Fraudegevoeligheid
- Communicatie

## 8 Uitbestedingsrisico

- Evaluatie
- Monitoring
- Selectie dienstverlener / verlengen contract
- IT risico externe organisatie

## 9 IT-risico

- Toegang IT interne organisatie
- IT bewustzijn interne organisatie
- IT beschikbaarheid, flexibiliteit en accuraatheid interne organisatie
- IT risico externe organisatie

## 10 Integriteitsrisico

- Onoorbaar handelen
- Belangenverstrengeling bij benoeming van leden van de organen
- Belangenverstrengeling algemeen

## 11 Juridisch risico

- Toetsing en evaluatie beleid, Wet- en regelgeving en naleving
- Aansprakelijkheid en afdwingbaarheid contracten

## 12 Beleidskader (risico overstijgende beheersingscategorieën)

- Solvabiliteitsbeheer

## Bijlage II: Beheersingskader

Monitoring van de beheersmaatregelen vindt plaats binnen een kader. Hiervoor worden acties opgesteld per risicocategorie en vastgelegd in de risicobeheer vastleggingstool. Het bestaan en de werking van de beheersmaatregelen wordt periodiek getoetst. Hiervoor gebruiken het fonds onderstaand beheersingskader.

| Frequentie  | Activiteit  |
|-------------|---|
| 3 jaarlijks | Evaluatie werking pensioenfondsbestuur (w.o. governance model, toekomstvisie structuur )  |
|             | Integrale ALM en evaluatie financiële opzet en beleggingsbeleid of indien aanleiding  |
|             | Eigen risico beoordeling: bij materiële wijzigingen in risicoprofiel een tussentijdse rapportage  |
|             | Evaluatie risico's van de gehanteerde beleggingsproducten en markten  |
|             | Evaluatiecyclus beleid (waar nodig vindt aanpassing van de documenten plaats)   |
|             | Evaluatie uitvoeringsovereenkomst: bij verlenging/wijziging inhoudelijke evaluatie. Bij voorstellen toets of fonds nog steeds binnen afspraken uitvoeringsovereenkomst werkt. |
| Jaarlijks   | Haalbaarheidstoets  |
|             | SIRA  |
|             | Evaluatie opzet en bestaan met herijking risicoraamwerk   |
|             | Vaststellen hoogte aansprakelijkheidsdekking (Jaarlijkse uitvraag: bij geen wijziging stilzwijgend verlengd)  |
|             | Opstellen herstelplan (indien van toepassing)   |
|             | Vaststelling jaarrekening en staten   |
|             | Toetsing wijzigingen wet- en regelgeving aan fondsdocumenten (w.o statuten / reglementen / overeenkomsten, en zo nodig aanpassingen doorvoeren)                               |
|             | Vaststelling begroting  |
|             | Vaststelling jaarplan op commissieniveau (bij CBM inclusief portefeuille constructie) en jaarplan op bestuursniveau   |
|             | Vaststelling communicatiejaarplan   |
|             | Evaluatie ABTN inclusief crisisplan (en zo nodig aanpassingen doorvoeren)   |
|             | Evaluatie functioneren organen fonds (bestuur, verantwoordingsorgaan en intern toezicht) / individuele gesprekken voorzitter/leden)   |
|             | Evaluatie uitbesteding (diensten uitbestedingspartijen)   |
|             | Rapportage compliance officer naleving gedragscode  |
|             | Rapportage privacy officer naleving privacybeleid   |
|             | Rapportage niet-financiële risico's aan DNB   |
|             | Analyse van ISAE 3402, ISAE 3000 en/of soortgelijke rapportages uitvoerders   |

| Frequentie           | Activiteit  |
|----------------------|---|
| Per kwartaal         | Kwartaalrapportage uitnutting begroting   |
|                      | Beoordeling effectiviteit risicoraamwerk, inclusief tweelijnsreview   |
|                      | Financiële kwartaalrapportage incl. informatie over aanwezige en benodigde solvabiliteit  |
|                      | Kwartaalrapportage pensioenadministratie en voorlichting in relatie SLA incl. klachtregister (rapportage niet-financiële risico's)                    |
|                      | Kwartaalrapportages vermogens- en onderpandbeheer in relatie tot SLA's en mandaten, incl. issue- en incidenten (rapportages niet-financiële risico's) |
|                      | IT Beheersingsrapportage Achmea IT  |
|                      | Dashboard Bestuur   |
|                      | Risico- en verantwoordingsrapportage commissies en bestuur  |
|                      | Incidentenrapportage  |
|                      | Rapportages sleutelfunctiehouders   |
|                      | Rapportage aan stakeholders   |
| Maandelijks          | Rapportage beleggingen op hoofdlijnen   |
|                      | Rapportage dekkingsgraad  |
| Wekelijks            | Weekrapport IT security   |
| Incidenteel terstond | Ingeval bestuursklachten, juridische casuïstiek   |
|                      | Ingeval issues, incidenten, meldingen en datalekken   |
|                      | Ingeval calamiteit (en zo nodig interventie in uitvoering / aanpassing beleid)  |

## Bijlage III: Scope van SIRA

De scope van de integriteitsrisico's in de SIRA is breder dan key controls uit bijlage 1.

Voor de SIRA hanteren wij de volgende integriteitsrisico's:

1. belangenverstremgeling (algemeen en benoeming bestuursleden)
2. fraudegevoeligheid (interne, externe en fiscale fraude)
3. witwassen
4. terrorismefinanciering
5. omzeiling sanctieregelgeving
6. corruptie (omkoping)
7. onoorbaar handelen (maatschappelijk onbetamelijk gedrag)
8. privacy
9. cybercrime
10. integriteit bij uitbesteding

## Bijlage IV: Begrippenlijst

- Wat is een risico en hoe is een risico te identificeren?

Een risico is iedere mogelijke gebeurtenis die van invloed is op het realiseren van de missie, visie, strategie en doelstellingen van het fonds. IRM is het middel om kansen en risico's en de beheersing daarvan af te stemmen op de missie, visie, strategie en doelstellingen van het fonds.

- Wat is een key performance indicator?

Een key performance indicator (KPI) meet hoe het fonds presteert op basis van de doelstellingen (missie en strategie) die het bestuur heeft vastgesteld, evenals de voortgang die wordt geboekt in de richting van deze doelen. KPI's worden gebruikt om de vraag te beantwoorden: bereiken we onze gewenste prestatieniveaus?

- Wat is een key control indicator?

Een key control indicator (KCI) is een indicator die meet hoeveel controle een bedrijf heeft over zijn omgeving en het risiconiveau. KCIs worden gebruikt om de vraag te beantwoorden: zijn de interne controles van onze organisatie effectief?

- Wat wordt verstaan onder risicobeheersing?

Beheersing van risico's draait niet om het uitsluiten van alle mogelijke risico's, maar om het vinden van een balans tussen kansen benutten (bewust risico's nemen) en bewust risico's verminderen, vermijden of overdragen. Hiertoe dient een afweging te worden gemaakt tussen de kosten en de opbrengst van risicobeheersing. Dit geldt voor zowel financiële als niet-financiële risico's.

- Wat wordt verstaan onder risicohouding?

De noodzakelijke mate van beheersing wordt bepaald door de risicohouding van het fonds. De risicohouding is de mate waarin het fonds bereid is bepaalde risico's te lopen om de missie, visie, strategie en doelstellingen te realiseren (risicobereidheid) en de mate waarin het fonds risico's kán lopen gegeven de kenmerken van het fonds (risicodraagvlak).

- Waarom is IRM een middel?

IRM is het middel dat zorgt voor optimale aansluiting tussen daadwerkelijke en gewenste blootstelling aan risico's. Het is daarmee tevens een middel bij het behalen van de missie, visie, strategie en doelstellingen en een middel om verantwoording af te leggen over gemaakte keuzes.

- Wat is het doel van IRM?

Het doel van IRM is in vier opeenvolgende acties te beschrijven:

- 1 Inzicht geven in de verschillende risico's
- 2 Inzichtelijk maken in welke mate risico wenselijk/acceptabel is
- 3 Overzicht bieden van de risico's om prioriteiten te kunnen stellen
- 4 Mogelijkheden bieden om de risico's te beheersen tot naar een wenselijk niveau

IRM is hiermee het middel om te zorgen dat de daadwerkelijke blootstelling aan risico's optimaal aansluit bij de wenselijke mate van blootstelling. Deze wordt bepaald vanuit de missie, visie, strategie en doelstellingen van het fonds.