Risicomanagementbeleid

10 maart 2025

SBZ Pensioen is een handelsnaam van Stichting Bedrijfstakpensioenfonds Zorgverzekeraars, kvk 41178751

Versiebeheer

Datum	Versie	Wie	Aanpassingen
08-02-2023	0.1	Vervuller SF RB	Conceptversie met wijzigingen t.o.v. het definitief risicomanagementbeleid d.d. 11 april 2022
10-02-2023	0.2	Vervuller SF RB	Aanvullingen vanuit de houder SF RB
28-02-2023	0.3	Vervuller SF RB	Aanvullingen vanuit KvdM
24-03-2023	0.4	Vervuller SF RB	- Aanvullingen vanuit UB - Toevoeging raamwerk transitierisico's WTP
07-04-2023	1.0	UB	Definitieve versie
23-01-2025	1.1	KvdM	Verwerken acties n.a.v. DORA assessment
05-01-2025	1.2	UB U&IT	Conceptversie gereed voor bespreking in ARC

Vaststelling

IJsselstein, 10 maart 2025

Namens het bestuur van SBZ Pensioen

Ties Tiessen
Voorzitter

Nienke Oosterheert
Uitvoerend bestuurder Uitbesteding & IT

Inhoud

1 Inleiding

1.1 Doel van dit document

Het risicomanagementbeleid beschrijft op hoofdlijnen hoe SBZ Pensioen risico's beheerst en de kaders die hiervoor bij het pensioenfonds en bij alle uitbestedingspartners gehanteerd worden. Het doel van dit document is om richting te geven en transparantie te verschaffen aan alle belanghebbenden in het kader van integraal risicomanagement binnen SBZ Pensioen.

1.2 Opbouw van dit document

Dit document is als volgt opgebouwd:

- Hoofdstuk 2 beschrijft de uitgangspunten van dit risicomanagementbeleid.
- Hoofdstuk 3 beschrijft de wijze waarop door SBZ Pensioen invulling wordt gegeven aan het risicomanagementraamwerk.
- Hoofdstuk 4 beschrijft de risico-governance van SBZ Pensioen.

2 Uitgangspunten risicomanagementbeleid

2.1 Definitie en doel risicomanagement

SBZ Pensioen definieert "risico" als de mogelijke afwijking van de ten doel gestelde uitkomsten. Afwijkingen kunnen impact hebben op:

- de waarde, het kapitaal of de inkomsten van SBZ Pensioen;
- de (gewezen) deelnemers, pensioengerechtigden of aangesloten werkgevers bij SBZ Pensioen;
- de organisatiedoelen of toekomstige mogelijkheden van SBZ Pensioen.

Risicomanagement betreft het identificeren en beoordelen van risico's, het vaststellen en implementeren van maatregelen en de bewaking en rapportage van risico's. Uitgangspunt hierbij is niet zozeer het uitsluitend voorkomen van risico's, maar juist het nemen van afgewogen besluiten over de te nemen risico's en de te nemen maatregelen bij het behalen van de strategische doelstellingen van SBZ Pensioen. Het behelst de strategie en het beleid met betrekking tot risico's en de kaders van het integraal risicomanagementraamwerk van het fonds bestaande uit procedures, richtlijnen, protocollen en instrumenten ten behoeve van het uitvoeren van het risicomanagementproces, ook als diensten zijn uitbesteed.

Hierbij wordt risicomanagement gebruikt als generieke term en omvat mede de compliance en de interne beheersing van SBZ Pensioen en de afzonderlijke uitbestedingspartners.

Het doel van risicomanagement is om de onzekerheid te managen van mogelijk optredende gebeurtenissen die het realiseren van de strategie in de weg kunnen staan. Voor een adequaat risicomanagement binnen SBZ Pensioen is het belangrijk dat er begrip en duidelijkheid is over de belangrijkste uitgangspunten ten aanzien van risicomanagement in de organisatie en dat er uniform en integraal naar wordt gehandeld. Als SBZ Pensioen tekortkomingen in de beheersing signaleert, dan worden aanvullende beheersmaatregelen (acties) ondernomen om de beheersing te versterken.

2.2 Uitgangspunten inrichting risicomanagement en risicocultuur

De visie van SBZ Pensioen op risicomanagement is de organisatie in staat te stellen om:

- De risico's te identificeren die de realisatie van de (strategische) doelstellingen kunnen bedreigen:
    - Het betreft de doelstellingen voor SBZ Pensioen, en
    - De doelstellingen bij de afzonderlijke uitbestedingspartners.[1]
- Kritische succesfactoren te formuleren vanuit de strategie, de risicobereidheid te bepalen inclusief meetbare key risk indicatoren (hierna KRI) en te sturen op de limieten van deze KRI.
- Een afgewogen geheel aan beheersmaatregelen voor het continu beheersen van de risico's samen te stellen, zodat het beheersingsniveau binnen de risicobereidheid van het fonds blijft, of indien dit niet realistisch is bewust en weloverwogen daarvan afwijkt.
- Bij het ongewenst optreden van een risico te zoeken naar de achterliggende oorzaken daarvan, mogelijke veranderingen te signaleren en daarop in te spelen met de juiste beheersmaatregelen.

De uitgangspunten ten aanzien van de inrichting van risicomanagement in de governancestructuur van SBZ Pensioen zijn:

- Risicomanagement is een integraal onderdeel van de processen. SBZ Pensioen kiest voor een integrale benadering bij het managen van risico's. Adequaat risicomanagement is onderdeel van de sturing van de organisatie (bij SBZ Pensioen en diens uitbestedingspartners).
- Risicomanagement is een integraal onderdeel van de besluitvorming. Besluitvorming is duidelijk, expliciet en in overeenstemming met de strategische doelstellingen en risicobereidheid van SBZ Pensioen. Besluitvorming is gebaseerd op een evenwichtige balans tussen risico en rendement.

[1] Middels het uitbestedings- en inkoopbeleid wordt geborgd dat de doelstellingen van de uitbestedingspartners in lijn zijn met de doelen van SBZ Pensioen. Grip op risicobeheersing is een voorwaarde bij uitbesteding.

- De governancestructuur van SBZ Pensioen is zodanig ingericht dat de onafhankelijkheid van het tweedelijns respectievelijk derdelijns risicomanagement ten opzichte van de eerste respectievelijk eerste en tweede lijn van SBZ Pensioen is gewaarborgd.
- Het bestuur van SBZ Pensioen stimuleert een open cultuur waarin risico's bespreekbaar zijn, bestuurders en medewerkers van uitbestedingspartners zich verantwoordelijk voelen om kennis te delen over risico's en waarin (pro)actief risicomanagement gewaardeerd wordt. Voorbeeldgedrag, bespreekbaarheid van dilemma's of uitvoerbaarheid van beleid, transparantie en aanspreekbaarheid zijn onlosmakelijk verbonden met de open cultuur evenals de mogelijke gevolgen bij het ontbreken daarvan.
- Risicomanagement is systematisch, gestructureerd en tijdig en gebaseerd op de best verkrijgbare informatie.
- Risicomanagement is dynamisch, iteratief, reageert op verandering, faciliteert continue verbetering.

Dit is nader uitgewerkt in hoofdstuk 4, waar de risico-governance aan de hand van het 3-lines of defence model is toegelicht. De risico-governance wordt jaarlijks beoordeeld door het bestuur van SBZ Pensioen om vast te stellen in hoeverre deze toereikend is ten aanzien van het ondersteunen bij het realiseren van de strategische doelstellingen van SBZ Pensioen.

2.3 Inbedding van het risicomanagementbeleid

De actuariële en bedrijfstechnische nota (Abtn) geeft de centrale criteria aan op basis waarvan het (financieel) beleid van SBZ Pensioen wordt gevoerd. In de Abtn komen alle aspecten van bedrijfsvoering, financieringsbeleid en risico's samen. Het is van belang om het beleid ten aanzien van diverse bedrijfsvoerings- en financieringsaspecten duidelijk vast te leggen. Dit heeft geleid tot diverse beleidsdocumenten naast de Abtn. Het beleid van SBZ Pensioen staat niet alleen in de Abtn, maar is concreter geformuleerd in de verschillende beleidsdocumenten.
Het (onderhavige) risicomanagementbeleid is er één daarvan. Het risicomanagementbeleid ziet ook op alle andere beleidsdocumenten van SBZ Pensioen.

Het risicomanagementbeleid identificeert de organisatiestructuur met betrekking tot risicomanagement en de hierbij behorende rollen en verantwoordelijkheden en beschrijft aspecten als de risicoclassificatie, de risicohouding en risicobereidheid en de bedrijfsvoering, onder te verdelen naar Instrumenten en technieken, Systemen en data, Mensen, cultuur en bewustzijn.

3 Integraal risicomanagementraamwerk

3.1 Algemeen

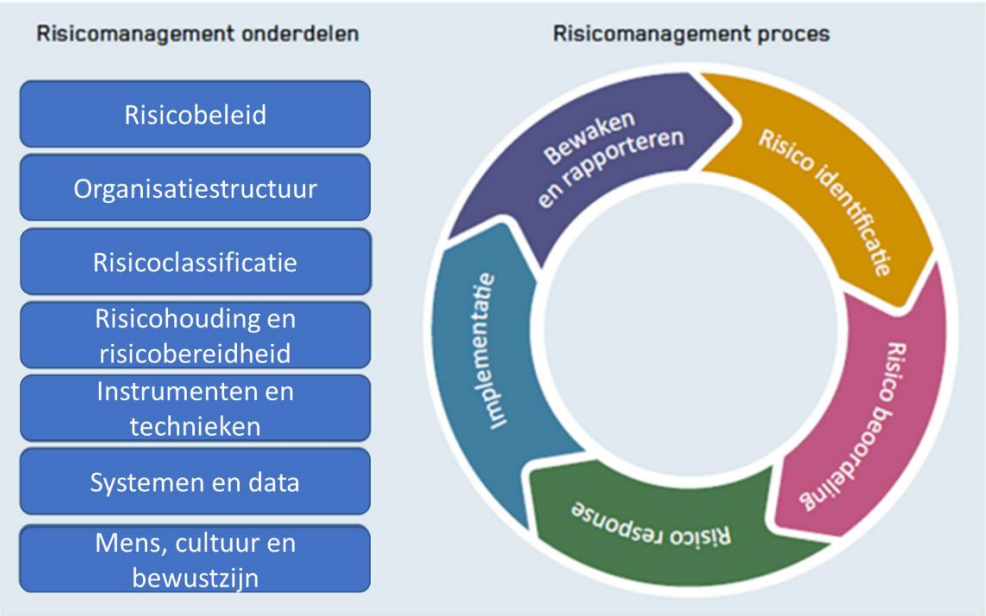
Integraal risicomanagement beoogt risicoprocessen, rapportages, methoden en technieken op elkaar te laten aansluiten en waar mogelijk te integreren. Door samenwerking en leereffecten tussen risicogebieden te bevorderen wordt de kwaliteit en toepassing van elkaars methoden en technieken verder verbeterd.

Het integraal risicomanagementraamwerk van SBZ Pensioen beschrijft het risicomanagementsysteem van SBZ Pensioen. Het raamwerk beschrijft hoe de risico's bij het pensioenfonds met behulp van een continu proces worden beheerst bij het streven naar de realisatie van de bedrijfsdoelstellingen. Het raamwerk draagt ertoe bij dat risico-informatie op een goede manier tot stand komt, wordt gerapporteerd en wordt gebruikt als basis voor besluitvorming en verantwoording. Ook ondersteunt het raamwerk SBZ Pensioen bij het effectief beheersen van haar risico's. Met integraal risicomanagement beoogt SBZ Pensioen een aantal doelstellingen te realiseren:

- *Kwaliteit besluitvorming*. Integraal risicomanagement zorgt ervoor dat het bestuur risico-gewogen informatie ontvangt, waarbij de inbreng van de second line of defence wordt meegewogen in de besluitvorming.
- *Bewuste risicosturing*. Integraal risicomanagement stelt SBZ Pensioen in staat om bewuster te sturen op risico's en risicospreiding. Welke risico's wil SBZ Pensioen nemen en welke vermijden?
- *Voorkomen over- en onderbeheersing*. Door interne beheersing explicieter te koppelen aan de risicobereidheid kan voorkomen worden dat SBZ Pensioen een raamwerk optuigt dat te zwaar of te licht is.

Het raamwerk is leidend bij de inrichting van het risicomanagement en borgt de onderlinge samenhang bij de verdere uitwerking en inrichting van de risico-governance.

Het raamwerk bestaat uit zeven risicomanagementonderdelen. Voor het borgen van kwaliteit wordt gewerkt met een cyclus voor het beheer van de verschillende onderdelen van het raamwerk. Voor een eenduidige benadering van de beheersing van risico's binnen SBZ Pensioen is daartoe een risicomanagementproces gedefinieerd. De onderdelen en het cyclische proces zijn in onderstaande figuur beschreven.



3.2 Risicomanagementonderdelen

3.2.1 Risicobeleid

Het risicobeleid ziet op het onderliggend beleid in relatie tot risicomanagement, de risicoprocedures en richtlijnen, die beschrijven op welke manier SBZ Pensioen de risico's voor elk risicotype beheerst. Voorbeelden van onderliggend beleid zijn het aansluitingenbeleid, het beleid collectieve waardeoverdrachten, het communicatiebeleid, het uitbestedings- en inkoopbeleid, het integriteitbeleid, het Business Continuity Management Beleid en het Beleid datakwaliteit.

Voor het beheer van de documenten op het gebied van risicomanagement en compliance is een beheercyclus ingericht onder verantwoordelijkheid van het uitvoerend bestuur van SBZ Pensioen. De documenten worden jaarlijks beoordeeld en indien nodig aangepast met het oog op elke substantiële verandering in de externe omgeving of het gebied dat het betreft. Wijzigingen worden vastgesteld door het Bestuur van SBZ Pensioen.

3.2.2 Organisatiestructuur

De organisatiestructuur beschrijft specifiek de organisatiestructuur van risicomanagement, de benodigde functies die daaraan gerelateerd zijn en het proces om deze te formaliseren.

SBZ Pensioen hanteert een opzet die voldoet aan de vereisten van IORP II. De organisatiestructuur en de rollen, verantwoordelijkheden en bevoegdheden zijn op hoofdlijnen beschreven in hoofdstuk 4 Risico-governance.

3.2.3 Risicoclassificatie

Risicocategorieën
SBZ Pensioen hanteert de risicotaxonomie van de Actualisatie Toezichtsmethodologie (ATM) van De Nederlandsche Bank (DNB). Hiermee sluit SBZ Pensioen aan op een in de pensioensector erkende categorisering. SBZ Pensioen hanteert, door de uniforme categorisering in het risicomanagement, een gemeenschappelijk taal in zowel het SLA-management met uitbestedingspartners als de verantwoording naar stakeholders. De binnen de ATM-risicotaxonomie door SBZ Pensioen onderscheiden risicocategorieën zijn in bijlage 1 nader toegelicht.

Risicoclassificatie (kwalitatief en kwantitatief)
De vastgelegde risicoanalyses voor SBZ Pensioen maken onderscheid tussen gebeurtenis, oorzaak en gevolg. Een gebeurtenis is iets dat kan voorvallen op een bepaald moment in de tijd. Iedere gebeurtenis heeft één of meerdere oorzaken. Een oorzaak is een omstandigheid die maakt dat iets ontstaat of begint en kan gedefinieerd worden als "een aanwezige omstandigheid die de kans op het vóórkomen van een gebeurtenis vergroot". Een gebeurtenis heeft altijd één of meerdere gevolgen. Gevolgen kunnen gedefinieerd worden als "de impact van een gebeurtenis op de organisatie". Gevolgen kunnen kwantitatief beschreven worden (bijvoorbeeld financiële schade), maar kunnen ook meer kwalitatief van aard zijn, zoals bijvoorbeeld reputatieschade.

In de risicoclassificatie worden zowel de bruto risico's (risico' zonder beheersmaatregelen) als de netto risico's (risico's inclusief beheersmaatregelen) op kans en impact gescoord. Hierbij wordt gewerkt met een vier-puntschaal (hoog, aanzienlijk, beperkt en laag). In bijlage 2 is deze methodiek nader toegelicht.

3.2.4 Risicohouding en risicobereidheid

De risicohouding van SBZ Pensioen beschrijft hoe het bestuur op een bepaald risico de balans ziet tussen risico en rendement. Risicohouding is het startpunt bij een besluitvormingsproces.

In het besluit financieel toetsingskader pensioenfondsen concentreert de risicohouding zich op de financiële risico's[2]. Op het gebied van niet-financiële bedrijfsvoering is vaststelling van de risicohouding even zo zeer relevant.
De risicohouding bij SBZ Pensioen kent vijf mogelijke niveaus:

Laag	Er worden geen risico's genomen, vanuit de visie dat gewenste rewards niet vereisen dat een minimaal niveau van blootstelling aan risico's wordt geaccepteerd.
Beperkt	De mate van blootstelling aan risico's wordt relatief laag gehouden, vanuit de visie dat gewenste rewards vereisen dat een relatief laag niveau van blootstelling aan risico's wordt geaccepteerd.
Gemiddeld	De mate van blootstelling aan risico's wordt gebalanceerd, vanuit de visie dat gewenste rewards vereisen dat een gebalanceerd niveau van blootstelling aan risico's wordt geaccepteerd.
Aanzienlijk	De mate van blootstelling aan risico's wordt relatief hoog gehouden, vanuit de visie dat gewenste rewards vereisen dat een relatief hoog niveau van blootstelling aan risico's wordt geaccepteerd.
Hoog	De blootstelling aan risico's is maximaal, vanuit de visie dat de gewenste rewards vereisen dat een maximale blootstelling aan risico's wordt geaccepteerd.

De risicohouding vormt het uitgangspunt voor het nader vaststellen van de risicobereidheid. De risicobereidheid wordt gedefinieerd als het maximum risico dat SBZ Pensioen kan en/of bereid is te accepteren bij het uitvoeren van de door haar gekozen doelstellingen. Met de risicobereidheid legt het bestuur vast wat nog wel acceptabel is en wat niet meer. Het gaat hierbij zowel om de hoogte van het risico (bedrag) als om het type risico.

Waar noodzakelijk geacht, worden op basis van risiconiveaus specifieke maatregelen geformuleerd, welke tenminste verplicht worden gesteld wanneer risico's buiten de risicobereidheid vallen. Geïmplementeerde maatregelen worden opgenomen in het risicobeheersraamwerk en de werking hiervan wordt getoetst en besproken in periodieke risicorapportages. Ter voorbeeld: encryptie en cryptografie als maatregel bij het transporteren en/of opslaan van (persoonsgevoelige) gegevens.

In de risicoclassificatie wordt de risicobereidheid uitgedrukt in termen van risicotolerantie op kans en impact. De risicokwantificatie is nader toegelicht in bijlage 2.

De risicobereidheid van SBZ Pensioen bepaalt vanuit een risicoperspectief de limieten waarbinnen SBZ Pensioen dagelijks opereert om haar doelstellingen te behalen. De risicobereidheid geldt als limiet, handvat en communicatiemiddel voor de besluitvorming en besturing van SBZ Pensioen.

SBZ Pensioen stelt per risico de risicohouding en risicobereidheid minimaal jaarlijks vast en actualiseert deze zo nodig.

De risicohouding en risicobereidheid zijn onderdeel van de reguliere risicobeoordeling die door het Uitvoerend Bestuur plaatsvindt (middels de risicoparagraaf). Daarmee vormen ze een leidraad voor de

[2] Artikel 1a van het Besluit financieel toetsingskader pensioenfondsen:

1 De risicohouding van een fonds, bedoeld in artikel 102a van de Pensioenwet dan wel artikel 109a van de Wet verplichte beroepspensioenregeling, is de mate waarin een fonds, na overleg met de vertegenwoordigers van werkgevers of werkgeversverenigingen, werknemers of werknemersverenigingen of beroepspensioenverenigingen en na overleg met de organen van het fonds, bereid is beleggingsrisico's te lopen om de doelstellingen van het fonds te realiseren en de mate waarin het fonds beleggingsrisico's kan lopen gegeven de kenmerken van het fonds.

2 De risicohouding van het fonds voldoet aan de prudent person regel en komt voor een uitkeringsovereenkomst of uitkeringsregeling voor de lange termijn tot uitdrukking in de door het fonds gekozen ondergrenzen in het kader van de haalbaarheidstoets en voor de korte termijn in de hoogte van het vereist eigen vermogen of een bandbreedte hiervoor.

3 Voor een premieovereenkomst, premieregeling of een variabele uitkering komt de risicohouding van het fonds tot uitdrukking in de door het fonds gekozen maximaal aanvaardbare afwijking van het pensioen in een pessimistisch scenario ten opzichte van het verwachte pensioen in een verwacht scenario. In de opbouwfase gaat het hierbij om het verwachte pensioen op pensioendatum; in de uitkeringsfase om afwijking van het pensioen van jaar op jaar. De risicohouding van het fonds voldoet aan de prudent person regel. De risicohouding wordt per toedelingskring vastgelegd.

risico-opinie vanuit de sleutelfunctie risicobeheer over de mate en kwaliteit van de risicobeheersing bij besluiten, die nieuw beleid of een wijziging van bestaand beleid inhouden.

De risicobereidheid vormt tevens de basis voor het uitvoeren van een goed risicomanagementproces dat met behulp van Key Performance Indicatoren (KPI) en Key Risk Indicatoren (KRI) gemeten wordt. Het vaststellen van KPI en KRI binnen SBZ Pensioen op het gebied van risico's is een belangrijke stap binnen het raamwerk van interne beheersing. Uitgangspunt hierbij is niet zozeer het voorkomen van risico's maar juist het nemen van weloverwogen besluiten over de te nemen risico's bij het behalen van de doelstellingen. Het hanteren van limieten of andere meetbare indicatoren geeft het bestuur houvast bij het sturen naar de optimale verhouding van risico en rendement.

De risicobereidheid dient voor het Bestuur van SBZ Pensioen als stuurmiddel bij haar strategische, tactische en operationele besluitvorming. Het Bestuur van SBZ Pensioen is en blijft eindverantwoordelijk voor de risicobereidheid van het fonds. SBZ Pensioen is zich ervan bewust dat situaties zich kunnen voordoen waardoor de risicobereidheid wordt overschreden. Op overschrijding dient bijsturing plaats te vinden. De KPI en KRI ondersteunen hierbij. Met behulp van deze KPI en KRI kan indien nodig tijdig worden bijgestuurd en kan worden voorkomen dat SBZ Pensioen aan risico's onder/boven de risicobereidheidsgrens wordt blootgesteld.

Het uitvoerend bestuur beoordeelt of SBZ Pensioen binnen de KPI en KRI blijft, informeert het niet-uitvoerend bestuur periodiek en doet aanbevelingen op basis van de resultaten van hun werkzaamheden. Het uitvoerend bestuur legt verantwoording af aan het niet-uitvoerend bestuur van SBZ Pensioen voor overschrijdingen. Het Bestuur is verantwoordelijk voor besluitvorming bij eventuele overschrijding van de risicobereidheid. Het Bestuur legt over de risicobereidheid verantwoording af aan het verantwoordingsorgaan.

Vaststelling en actualisering van de KPI en KRI is onderdeel van het jaarplan IRM.

3.2.5 Instrumenten en technieken

Instrumenten en technieken bieden per risicotype concrete en praktische ondersteuning om het risicoproces uit te voeren. De uitkomsten van de verschillende risicoanalyses en de toetsing aan de risicobereidheid, geven richting aan de risico's waarvoor aanvullende beheersingsmaatregelen moeten worden genomen. Deze aanvullende beheersingsmaatregelen worden vertaald in acties, waarvan de voortgang wordt bewaakt. In paragraaf 3.3 is verder aandacht voor de implementatie en monitoring van de voortgang op deze acties.

Risicomanagementaanpak
SBZ Pensioen maakt gebruik van een integrale risicomanagementaanpak voor pensioenfondsbesturen gebaseerd op de ATM. Met deze aanpak wordt voldaan aan de door DNB gevraagde minimale volwassenheidsniveaus voor risicomanagement[3]: Het fonds hanteert een gestructureerde aanpak, die aantoonbaar door de hele organisatie (SBZ Pensioen en diens uitbestedingspartners) wordt gevolgd en waarin beheersmaatregelen periodiek worden beoordeeld op effectiviteit en zo nodig aangepast.

Eigen risicobeoordeling (ERB)
Voor de inrichting van het risicobeheer en de onderbouwing van strategische besluitvorming is de ERB van essentieel belang. De ERB geeft inzicht in de materiële risico's en de mogelijke consequenties

[3] Voor volwassenheidsniveau 4 wordt vereist:
- RM-functie (AO) is ingericht en schriftelijk vastgelegd. RM-functie is ingericht en wordt aantoonbaar aangestuurd door het verantwoordelijke bestuurslid.
- RM is vast agendapunt. Besluiten en bestuursoverwegingen mbt RM worden vastgelegd.
- De risicostrategie is afgeleid van de (generieke) missie/strategie fonds. Het beleid is autonoom door het bestuur opgesteld (maatwerk/onafhankelijk van adviseurs). Invulling risicobereidheid per categorie en integraal gedaan. Het beleid is op schrift gesteld en door het bestuur formeel bekrachtigd. Er vindt adequate actualisering en periodieke communicatie plaats.
- Het bestuur is in de drivers seat. Bij gebruik adviseurs zijn die aantoonbaar onafhankelijk.
- Risicorapportages worden periodiek en aantoonbaar besproken in het bestuur en met de stakeholders.

hiervan voor de financiële positie van het pensioenfonds en de pensioenen van deelnemers. Het fonds beoordeelt daarmee periodiek de effectiviteit en de doelmatigheid van het risicobeheer.

De ERB maakt integraal onderdeel uit van de strategie en het risicobeheer. SBZ Pensioen voert tenminste driejaarlijks een reguliere 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).
2. Strategisch besluit met een materiële impact op het risicoprofiel.

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

Structurele risicoanalyses
Belangrijke instrumenten binnen de aanpak zijn de risicoanalyses. Risicoanalyses geven sturing aan het in kaart brengen en managen van risico's om ongewenste directe en indirecte gevolgen te voorkomen. Risicoanalyses zijn daarmee een hulpmiddel om de doelstellingen van SBZ Pensioen te realiseren en zijn daarmee belangrijke bouwstenen van een geïntegreerd risicobeheersysteem.

SBZ Pensioen vindt het belangrijk dat risicoanalyses effectief, efficiënt en op uniforme wijze plaats vinden, zodat een adequaat risicobeeld opgebouwd kan worden, inclusief de risico's van uitbestedingspartners, waarop het bestuur van SBZ Pensioen stuurt.

Om dit adequaat uit te voeren:

- stelt SBZ Pensioen jaarlijks een jaarplan op voor de risico-inventarisatie; dit plan gaat in op het "wat" en op het "hoe" waarin aandacht is voor de processtappen voorbereiding, risico-identificatie, risicobeoordeling, risicorespons, rapportage-uitkomsten en bewaking van de risicobereidheid;
- vindt de beoordeling van de risico's plaats in overeenstemming met de risicocategorieën en risicoclassificatie en vindt vastlegging plaats in een gekwantificeerde risicoanalyse;
- vindt rapportage over de uitkomsten, inclusief voorstellen voor verbetering van de beheersing plaats aan het bestuur;
- vindt interactie plaats tussen het uitvoerend deel van het bestuur van SBZ Pensioen en de (tweede lijn functionarissen van de) uitbestedingspartners.

Het bestuur van SBZ Pensioen is verantwoordelijk voor het initiëren en houden van risicoanalyses. Het uitvoerend bestuur bereidt de beleidskaders voor, ondersteunt, bewaakt, rapporteert en indien nodig escaleert.

(Risico)rapportages van uitbestedingspartners
De eisen die aan uitbestedingspartners worden gesteld zijn vastgelegd in het uitbestedings- en inkoopbeleid van SBZ Pensioen. Van de uitbestedingspartners wordt op het gebied van risicomanagement verwacht dat zij:

- zijn ingericht in overeenstemming met het 'Three Lines of Defence'-model van het Institute of Internal Auditors;
- risicomanagement een belangrijke rol geven in de organisatie;
- een integraal risicomanagementraamwerk hebben ingericht, waaronder instrumenten en technieken;
- over risicomanagement rapporteren aan SBZ Pensioen.

Aan de kritieke en belangrijke uitbestedingspartners worden normen gesteld ten aanzien van de rapportages, die aan SBZ Pensioen worden verstrekt, en de periodiciteit en proportionaliteit hiervan. Het uitvoerend bestuur van SBZ Pensioen beoordeelt de kwaliteit van deze rapportages en rapporteert dit aan het Bestuur van SBZ Pensioen.

Incidentele risicoanalyses

Naast het reguliere ingerichte proces kunnen er andere triggers zijn om een risicoanalyse te plannen die meer incidenteel van aard is. Niet limitatief kunnen deze komen uit:
- wijzigingen op het gebied van wet- en regelgeving;
- verzoeken van het bestuur of verantwoordingsorgaan;
- inzet van nieuwe uitbestedingspartners of systemen door SBZ Pensioen;
- externe factoren, waaronder inzet van nieuwe systemen of onderuitbestedingspartners door uitbestedingspartners van SBZ Pensioen;
- issues vanuit het issuemanagement;
- incidenten;
- rapportages van de uitbestedingspartners of periodieke gesprekken met de (tweede lijn functionarissen van de) uitbestedingspartners;
- het bewaken van de KRI door het uitvoerend deel van het bestuur van SBZ Pensioen.

Risicoparagrafen bij bestuursbesluiten
Het bestuur hanteert het BOB-model. BOB staat voor Beeldvorming – Oordeelsvorming – Besluitvorming. Het doel van Beeldvorming is zoveel mogelijk informatie te verzamelen om te komen tot een heldere probleemdefinitie. Bij Oordeelsvorming worden verschillende oplossingen bedacht voor het probleem en criteria opgesteld op basis waarvan de verschillende oplossingen worden beoordeeld. Bij Besluitvorming vindt de keuze van een oplossing op basis van de criteria opgesteld in Oordeelsvorming plaats, inclusief de planning en uitvoering van het besluit.
Besluitvorming wordt voorzien van een risicoparagraaf. In de risicoparagraaf worden met betrekking tot de risico's die door het besluit worden geraakt de risicohouding, de risicobereidheid, de aanwezige risicobeheersing en de eventueel aanvullend vereiste risicobeheersing benoemd. De risicoparagraaf wordt betrokken in de besluitvorming.
Bij besluiten, die nieuw beleid of een wijziging van bestaand beleid inhouden, geeft de Sleutelfunctiehouder Risicobeheer via een onafhankelijke risico-opinie zijn/haar mening over de risicoparagraaf.

3.2.6 Systemen en data

Informatiebeveiliging en cybersecurity zijn een integraal onderdeel van de IT-risicobeheersing door het fonds. Er wordt daarom expliciet aandacht besteed aan informatiebeveiligings- en cybersecurity risico's door middel van het doorlopen van de reguliere managementcyclus en het security awareness programma ten behoeve van het verhogen van het bewustzijnsniveau van SBZ.

SA DNB IB Good Practice
Jaarlijks vult SBZ Pensioen het DNB Good Practice informatiebeveiliging (hierna: DNB GP IB) Self Assessment in voor de voor het fonds relevante controls. Hiermee geeft SBZ Pensioen inzicht aan DNB in de beheersing van de voor het fonds relevante onderwerpen ten aanzien van informatiebeveiliging. Het Uitvoerend Bestuur voert met ondersteuning van de SFH Risicobeheer, en eventuele additionele benodigde expertise, het assessment uit. Eventuele gesignaleerde verbeterpunten worden opgepakt en opgelost binnen de managementcyclus.

*IT-risicoanalyse*Onderdeel van de structurele risicoanalyses betreft het in kaart brengen van de belangrijkste processen van SBZ Pensioen en de proceseigenaar. Dit betreft zowel de processen in eigen beheer als de processen die zijn uitbesteed[4]. Voor het in kaart brengen van de IT-risico's wordt vanuit de processen gedacht en de ondersteunende IT-keten in kaart gebracht.
Van de IT-keten worden de kritieke en belangrijke systemen geïdentificeerd. Per proces wordt bepaald welke eisen worden gesteld aan de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de data. Deze eisen worden doorvertaald naar de systemen die (door de uitbestedingspartner) worden ingezet om de processen uit te voeren. Hierbij is het mogelijk om per systeem van het proces afwijkende BIV-eisen te formuleren. Op de systemen worden aanvullend op de BIV-eisen ook eisen gesteld aan de aanpasbaarheid van het systeem.

[4] In het uitbestedings- en inkoopbeleid wordt het doel, de reikwijdte en het proces van uitbestedingen beschreven. In de bij het uitbestedings- en inkoopbeleid behorende Bijlage 9 worden aanvullende eisen gesteld voor uitbestedingen van IT-systemen en/of software die ter ondersteuning van de algehele bedrijfsvoering worden ingezet.

Business Impact Analyse (BIA)
Volgend uit de IT-risicoanalyse stelt het Uitvoerend Bestuur met ondersteuning van de SFH Risicobeheer, en eventuele additionele benodigde expertise middels een BIA de processen en bedrijfsactiviteiten vast die kritiek zijn voor het behalen van de doelstellingen van SBZ Pensioen. Dit bevat ook de processen die zijn uitbesteed. De uitkomsten geven richting aan SBZ en haar uitbesteders welke processen allereerst hersteld dienen te worden of beschermd dienen te worden tegen uitval.

Diverse aandachspunten ten aanzien van systemen en data hebben geleid tot beleidsvorming om geïdentificeerde risico's binnen het fonds te addresseren. Hiermee zijn de onderliggende risico's en beheersing hiervan onderdeel van de managementcyclus van SBZ pensioen, en worden daarmee structureel geborgd binnen het bestuur. Dit betreft:

- IT-beschikbaarheid: Business Continuity Management Beleid
- IT-integriteit: Beleid datakwaliteit

3.2.7 Mensen, cultuur en bewustzijn

Mensen, cultuur en bewustzijn betreffen de aspecten die in mensen zitten en die ten goede komen aan adequaat risicomanagement.

Het bestuur draagt zorg voor haar eigen deskundigheid en geschiktheid, zodat het voldoende 'coutervailing power' heeft ten opzichte van operationele activiteiten en uitbestedingspartijen. Dit is onderdeel van het geschiktheidsplan dat het fonds heeft opgesteld. Geschiktheid wordt binnen het bestuur gewaarborgd door per vacante positie passende geschiktheidseisen vast te stellen, rekening houdend met de kennis en expertise van de zittende leden. Daarnaast wordt beoordeeld of de kennis van de zittende leden nog voldoende actueel is. Om de kennis op peil te houden of te brengen worden opleidingsmogelijkheden geboden. Indien het bestuur van mening is dat deskundigheid en/of geschiktheid tekortschiet, zal het bestuur altijd besluiten externe expertise in te zetten. Daarnaast is deskundigheid en geschiktheid van medewerkers onderdeel van de jaarlijkse evaluatie die SBZ Pensioen houdt met uitbestedingspartners en adviseurs.

Voor SBZ Pensioen speelt cultuur een essentiële rol in adequaat risicomanagement. De structuur van risicomanagement moet adequaat worden ingevuld, maar het gedrag en de naleving van afspraken kenmerken een risicocultuur in een organisatie en bepalen mede de effectiviteit van risicomanagement. Verantwoordelijkheid nemen en verantwoordelijkheid afleggen, handelen in de geest van de wet, evenwichtig en consistent handelen, informatiebeveiliging en cybersecurity zijn een zaak van iedereen. Open communicatie, het melden van zwakheden en incidenten zijn bepalend voor de cultuur. Cultuur is minder eenvoudig te meten, maar communicatie van uitgangspunten en voorbeeldgedrag ten aanzien van deze uitgangspunten zijn voor de risicocultuur bepalend.

Culturele aspecten en risicobewustzijn worden gestimuleerd door:

- Het een vast onderdeel laten zijn van de bestuurskalender en/of bestuursagenda van bijvoorbeeld risicorapportages of voortgangsrapportages.
- Het invullen van studiedagen waarbij relevante ontwikkelingen, bijvoorbeeld op het gebied van wet- en regelgeving, fraude, informatiebeveiliging en cybersecurity en actualiteiten worden behandeld.
- Incidenten formeel vast te leggen in een incidentenregister, waarbij bij de classificatie van incidenten expliciet aandacht wordt besteed aan de oorzaak.

De verwachte niveaus van integriteit, ethisch handelen en deskundigheid worden expliciet gemaakt (ook naar de uitbestedingspartners) waarbij individuen kunnen aangesproken worden op het ondersteunen en onderhouden van een cultuur gebaseerd op integriteit.
Kennis en vaardigheden die nodig zijn om de toegewezen taken uit te voeren zijn duidelijk beschreven in functieprofielen die binnen SBZ Pensioen worden gehanteerd. In de performancecyclus worden deze functieprofielen gebruikt om alle individuen op performance te beoordelen.

Minimaal jaarlijks vindt door het bestuur van SBZ Pensioen beoordeling plaats van de cultuur- en bewustzijns-oorzaken van belangrijke afwijkingen. Op basis van de analyse worden jaarlijks

risicobewustzijn programma's opgesteld. De acties uit de programma's worden uitgevoerd en over de uitkomsten wordt gerapporteerd aan het bestuur.

In de monitoring op haar uitbestedingspartners door SBZ Pensioen maakt risicocultuur onderdeel uit van de beoordeling.

3.3 Risicomanagementproces

Het risicomanagementproces kijkt vooruit en is in de organisatiestructuur en in de besluitvormingsprocessen van SBZ Pensioen geïntegreerd.

Het risicomanagementproces ondersteunt de noodzakelijke stappen om risico's van alle risicotypes continu te identificeren, te beoordelen, te beheersen, te bewaken en te rapporteren. De stappen in het risicomanagementproces zijn:

- Risico-identificatie: het op basis van de strategie en doelstellingen identificeren van de potentiële risico's die de realisatie van de strategie en doelstellingen kunnen belemmeren.
- Risicobeoordeling: het analyseren, beoordelen en mogelijk kwantificeren van de (oorzaken van de) risico's.
- Risicoresponse: het bepalen van de maatregelen om met het risico om te gaan, waarbij opties zijn:
  - risicovermijding (stoppen met activiteiten),
  - risico-acceptatie (geen maatregelen),
  - risicobeheersing (beheersingsmaatregelen / controls), of
  - risico delen (herverzekeren)
- Implementatie: het daadwerkelijk inrichten, implementeren en verankeren van de maatregelen, het opvolgen van openstaande acties, het uitvoeren van cultuuraspecten (bewustwordingsprogramma, incidentenregistratie en bespreken in het bestuur). Indien het niet haalbaar is om beheersmaatregelen of activiteiten zoals beschreven in beleid te implementeren, moet een expliciete risico acceptatie en de duur daarvan door het UB voorgelegd worden aan de ARC ter advisering, alvorens het Bestuur hierover besluit.
- Bewaken & rapporteren: het gedurende het gehele risicomanagementproces bewaken en verantwoording afleggen over de kwaliteit van de beheersing en voortgang van de verbeteringen aan het bestuur. De rapportages van uitbestedingspartijen aan SBZ Pensioen en de uitkomsten van audits, testen en oefeningen vallen hier onder. Het bestuur besluit over de verbetervoorstellen in de rapportages en neemt de genomen besluiten op in de periodieke monitoring.

Er zijn interne en externe analyses en rapportages beschikbaar waarmee inzicht wordt gegeven in het risicoprofiel en de beheersing van de risico's. Waar nodig wordt aanvullend gerapporteerd in separate rapportages over specifieke onderwerpen. Voor deze rapportages geldt dat de totstandkoming van deze rapportages een integraal onderdeel uitmaakt van het risicomanagementproces van SBZ Pensioen.

In onderstaande tabel is een overzicht gemaakt van de rapportages:

Volledige naam en titel	Inhoud	Frequentie
Risico- en overige rapportages uitbestedingen *(van uitbestedingspartners, aan uitvoerend bestuur)*	Integrale beoordeling van de risico's van een uitbestedingspartij. Een belangrijk overzicht vanuit deze analyse is een lijst met belangrijke risico's van de uitbestedingspartij in het kader van de uitbesteding van SBZ Pensioen. Daarnaast wordt o.a. gerapporteerd over (de afhandeling van) incidenten.	Kwartaal
ISAE 3402/3000 Type 2 of vergelijkbaar *(van uitbestedingspartners, aan bestuur*)	De uitbestedingspartner levert conform de uitbestedings-overeenkomst de jaarlijkse ISAE 3402 /3000 Type 2 rapportage (of vergelijkbaar) zodat SBZ Pensioen structureel geïnformeerd is over het risicomanagement, de beheersmaatregelen en naleving daarvan.	Jaarlijks
Rapportages operationeel risicobeheer	Informatie vanuit het uitvoerend bestuur over de risicopositie van SBZ Pensioen, inclusief risico's bij de kritische en belangrijke uitbestedingspartijen. Aan de	Kwartaal

(van uitvoerend bestuur, aan niet-uitvoerend bestuur)	gerapporteerde risico's wordt een duiding toegevoegd waarin wordt afgewogen in hoeverre gerapporteerde risico's voor SBZ Pensioen buiten de risicotolerantie liggen. Indien een gerapporteerd risico voor SBZ Pensioen buiten de risicotolerantie ligt kunnen voorstellen voor acties vanuit SBZ Pensioen richting de uitbestedingspartijen benoemd worden. Onderdeel van de rapportage is de rapportage operationeel risicobeheer, waarin ook acties vanuit SBZ Pensioen richting de uitbestedingspartijen op basis van de risico- en overige rapportages van deze partijen benoemd worden. Daarnaast is er aandacht voor incidenten en de voortgang van de uitvoering van de verbeterplannen m.b.t. de belangrijkste risico's.	
Haalbaarheidstoets *(van uitvoerend bestuur, aan bestuur)*	Informatie over het integrale risicoprofiel en een projectie van de actuele en geprojecteerde vereisten en het beschikbare kapitaal voor de komende jaren, waarbij tevens een toetsing is opgenomen of het beschikbare kapitaal afdoende is gegeven het risicoprofiel.	Jaarlijks en bij belangrijke wijzigingen in risicohouding
ALM-studie *(van uitvoerend bestuur, aan bestuur)*	Informatie over de onderlinge afhankelijkheden in de ontwikkeling van het vermogen en de verplichtingen van SBZ Pensioen (bezien vanuit de regeling, premie, toeslagen en beleggingen).	2-Jaarlijks
Risicomanagement-paragraaf van de jaarrekening *(van uitvoerend bestuur, aan niet-uitvoerend bestuur)*	Beschrijving van het integrale risicomanagement van SBZ Pensioen.	Jaarlijks
Accountantsverslag *(van controlerend accountant, aan bestuur)*	Gedetailleerde informatie vanuit de accountant in het kader van de jaarrekening.	Jaarlijks
Rapport waarmerkend actuaris *(van waarmerkend actuaris, aan bestuur)*	Gedetailleerde informatie vanuit de waarmerkend actuaris in het kader van de jaarrekening.	Jaarlijks
Actuariële rapportage *(van actuariële functie, aan bestuur)*	Rapportage vanuit de sleutelfunctie actuarieel. Indien van toepassing bevat de rapportage bijsturingsvoorstellen.	Kwartaal
Risicorapportage *(van risicobeheerfunctie, aan bestuur)*	Rapportage vanuit de sleutelfunctie risicobeheer. Indien van toepassing bevat de rapportage bijsturingsvoorstellen.	Kwartaal
Interne audit rapportage *(van interne audit functie, aan bestuur)*	Rapportage vanuit de sleutelfunctie interne audit. Indien van toepassing bevat de rapportage bijsturingsvoorstellen.	Kwartaal
Rapportage compliance en privacy *(van compliance officer en functionaris gegevensbescherming, aan bestuur)*	Rapportage over compliance en privacy gerelateerde zaken (onder meer de maatregelen die genomen zijn in het geval zich tekortkomingen hebben voorgedaan). Indien van toepassing bevat de rapportage bijsturingsvoorstellen.	Jaarlijks

Het bestuur van SBZ Pensioen evalueert minimaal jaarlijks het risicomanagementproces aan de hand van het IRM jaarplan en de rapportages operationeel risicobeheer vanuit het uitvoerend bestuur, de risicorapportages vanuit de sleutelfunctie risicobeheer en de interne audit rapportages vanuit de sleutelfunctie interne audit. Bij de evaluatie worden (operationele) incidenten meegenomen.

Naast het risicomanagementproces wordt ook het risicomanagementbeleid en de opzet van de risico governance minimaal driejaarlijks als onderdeel van de Eigen Risico Beoordeling (ERB) geëvalueerd. De evaluatie wordt gedocumenteerd in de eindrapportage ERB en door het bestuur vastgesteld.

De opzet en uitvoering van het risicomanagementproces, het risicomanagementbeleid en de risico-governance wordt door het bestuur geëvalueerd om vast te stellen in hoeverre deze toereikend is ten aanzien van het ondersteunen bij het realiseren van de strategische en operationele beheersingsdoelstellingen van SBZ Pensioen.

Bij de evaluatie benoemde verbeterpunten worden zichtbaar opgevolgd.

4 Risico-governance

4.1 Three Lines of Defence

Kort samengevat houdt het ‘Three Lines of Defence’-model het volgende in:

1) De 1e lijn betreft het management en de medewerkers in de lijn die de beheersmaatregelen in de processen uitvoeren.
2) De 2e lijn, Risk Control en Compliance, stelt vervolgens vast in welke mate de beheersmaatregelen hebben gewerkt. Zij ondersteunen en adviseren de 1e lijn en bewaken of de 1e lijn zijn verantwoordelijkheden op het gebied van beheersing ook daadwerkelijk neemt. Ook bepaalde beleidsvoorbereidende taken (het opzetten van het risicobeheerraamwerk) en de coördinatie van het proces van risicobeheersing, waaronder het organiseren van integrale risk assessments zijn taken van de 2e lijn. Daarnaast houden zij zicht op de werking van het proces en de gerealiseerde beheersingsniveaus.
3) De 3e lijn, Interne Audit, stelt, in samenwerking met de 4e lijn, de Externe Accountant en de Certificerend Actuaris, tot slot vast dat de administratieve organisatie en interne controlesystemen in de 1e lijn bestaan en werken en dat de 2e lijn de werking van de financiële en niet-financiële risicobeheersmaatregelen daadwerkelijk goed heeft getest. Daarmee komt zij tot een onafhankelijk oordeel over de mate waarin er sprake is van een aantoonbare effectieve risicobeheersing.

Dit onderscheid draagt bij aan een beter begrip van integraal risicomanagement en geeft handvatten bij het onderscheiden van taken en verantwoordelijkheden.

SBZ Pensioen blijft verantwoordelijk voor de uitvoering van haar risicomanagement bij de verschillende uitbestedingen. Hiertoe maakt SBZ Pensioen ten behoeve van een beheerste uitbesteding afspraken met haar uitbestedingsrelaties en andere dienstverleners over het werken in overeenstemming met dit Risicomanagementbeleid en de geformuleerde risicobereidheid. Deze afspraken werken door in eventuele onderuitbestedingen. Het uitbestedings- en inkoopbeleid gaat hier verder op in.

In de organisatie van SBZ Pensioen als pensioenfonds zijn aanvullende maatregelen genomen om de beheersing van risico’s te organiseren. Ook die organisatie heeft de vorm van drie verdedigingslagen en kan dan ook beschouwd worden als The Three Lines of Defence van SBZ Pensioen zelf.

Ook hier betreft de 1e lijn het operationeel management: het uitvoerende deel van het bestuur dat verantwoordelijk is voor het beheerst uitvoeren van zijn eigen processen (waaronder het zicht houden op de risicobeheersing van de uitbestedingspartners). Ook het inrichten en uitvoeren van het risicomanagementproces is de verantwoordelijkheid van het uitvoerend bestuur.

Daarnaast vormen de Sleutelfunctiehouder Actuarieel, de Sleutelfunctiehouder Risicobeheer, de Compliance Officer en de Functionaris Gegevensbescherming de 2e lijn.

Het risicobeheer bij uitbestedingspartijen valt onder de verantwoordelijkheid van de 1e lijn door gebruik te maken van de rapportages. De eerste lijn wordt hierbij ondersteund door de functionarissen in de 2e lijn. Indien daar aanleiding toe is kan er gezamenlijk (1e en 2e lijn) worden overlegd met de 2e lijn bij deze partijen.

De 3e lijn tot slot wordt gevormd door de Sleutelfunctiehouder Interne Audit. Hij/zij ziet toe op de interactie tussen de 1e en 2e lijn en bewaakt of de 1e en 2e lijn hun verantwoordelijkheden ook daadwerkelijk nemen. Bovenstaande strekt zich ook uit over de werkzaamheden met betrekking tot de uitbestedingspartijen. Hij/zij kan bij zijn/haar werkzaamheden gebruik maken van Externe Accountantsonderzoeken. Hiervoor zal de Sleutelfunctiehouder Interne Audit ten behoeve van het Bestuur een Meerjaren Auditplan opstellen, waaruit een audit jaarplan resulteert. Tevens heeft de Sleutelfunctiehouder Interne Audit een Auditcharter, die periodiek wordt geëvalueerd.

4.2 Niet-uitvoerend deel van het bestuur

Het intern toezicht is belegd bij het Niet-Uitvoerend Bestuur. De Niet-Uitvoerende Bestuursleden houden toezicht op:

a. de uitvoering van het beleid door de Uitvoerende Bestuursleden;
b. de algemene gang van zaken in het fonds;
c. adequate risicobeheersing en evenwichtige belangenafweging.

De Niet-Uitvoerende Bestuurders leggen over hun toezichtstaken verantwoording af aan het Verantwoordingsorgaan.

Naast de rol als toezichthouder vervult het Niet-Uitvoerend Bestuur nog een aantal andere rollen. Voor de Uitvoerende Bestuurders treedt het Niet-Uitvoerend Bestuur op als werkgever in de beoordeling van hun functioneren, het vaststellen van hun beloning, maar ook in hun terzijde staan van raad. Tenslotte is het Niet-Uitvoerend Bestuur actief in het beheer van de externe relaties ("stakeholdermanagement").

Ontheffing auditcommissie
Bij de overgang naar het omgekeerd gemengd bestuursmodel heeft DNB aan SBZ Pensioen ontheffing verleend voor het instellen van een auditcommissie op grond van de binnen het bestuur van SBZ Pensioen aanwezige deskundigheid ten aanzien van het toezicht op de risicobeheersing, het beleggingsbeleid en de financiële informatieverschaffing door het fonds.
In 2017 heeft DNB gevraagd aan het bestuur om te borgen dat er voldoende kennis en deskundigheid is binnen het bestuur en de Audit- Risk en Compliancecommissie en alleen melding te doen als er een gedegen aanleiding is. Bij een wijziging in de samenstelling van het bestuur of de Audit- Risk en Compliancecommissie wordt DNB volgens de gebruikelijke procedures geïnformeerd. Indien het bestuur van mening is dat kennis en deskundigheid in de nieuwe samenstelling voldoende is op de toezichtsgebieden waarvoor een auditcommissie verantwoordelijk is, wordt gemeld dat bij geen tegenbericht van DNB ervanuit wordt gegaan dat de ontheffing wordt verlengd.

Commissies
Het Niet-Uitvoerend Bestuur laat zich in de uitvoering van haar taken bijstaan door drie (vaste) Bestuurlijke commissies:

- Een Audit- Risk- en Compliancecommissie (met name ten behoeve van (advisering over) de monitoring van de pensioenuitvoering en jaarverslaglegging, compliance en risicobeheersing en intern toezicht). Deze commissie bestaat in beginsel uit drie Niet-Uitvoerende Bestuursleden. De taken en bevoegdheden van deze commissie zijn vastgelegd in het Reglement Audit- Risk- en Compliancecommissie.
- Een BeleggingsAdviescommissie (met name ten behoeve van de advisering over en monitoring van de uitvoering van het beleggingsbeleid). Deze commissie bestaat in beginsel uit drie Niet-Uitvoerende Bestuursleden aangevuld met Externe adviseurs. De taken en bevoegdheden van deze commissie zijn opgenomen in het Reglement BeleggingsAdviescommissie, evenals in het Strategisch Beleggingsbeleid.
- Een Commissie Bestuurlijke Aangelegenheden die adviseert over een adequate personele bezetting van het de Bestuurlijke gremia, waaronder begrepen ook de opvolging, de beloning en de rol van de Niet-Uitvoerende Bestuursleden als intern toezichthouder waarbij ze voorbereidende taken voor de vergadering van het Niet-Uitvoerende deel van het Bestuur krijgt. Deze commissie bestaat uit de voorzitter van de Audit- Risk- en Compliancecommissie, de voorzitter van de BeleggingsAdviescommissie en een Niet-Uitvoerend Bestuurslid dat de voorzitter van de Commissie Bestuurlijke Aangelegenheden wordt. De taken en bevoegdheden van deze commissie zijn vastgelegd in het Reglement Commissie Bestuurlijke Aangelegenheden.

De commissies kennen:

- vaste genodigden:
    - voor de Audit-, Risk- en Compliancecommissie is dit het Uitvoerend Bestuurslid Pensioenen en Risicobeheer;
    - voor de BeleggingsAdviescommissie is dit het Uitvoerend Bestuurslid Beleggingen en Vermogensbeheer;
    - voor de Commissie Bestuurlijke Aangelegenheden is dit de Onafhankelijk Voorzitter.

- incidentele genodigden:
    - het Uitvoerende Bestuurslid dat geen vaste genodigde is;
    - de Onafhankelijk Voorzitter;
    - de Sleutelfunctiehouders Risicobeheer, Actuarieel en/of Interne Audit;
    - deskundigen van de uitbestedingspartners;
    - eventuele andere externe deskundigen.

De commissies en het Niet-Uitvoerende deel van het Bestuur hebben als informatiebronnen de verantwoording door het Uitvoerende deel van het Bestuur (mede door middel van de risicorapportage Uitvoerend Bestuur) , de SLA-rapportages, de aanvullende rapportages vanuit de 2e lijn van de uitvoeringsorganisaties en de jaarlijkse ISAE rapportages van de uitvoeringsorganisaties. En ter finale bevestiging krijgen zij de rapportages van de Sleutelfunctiehouders en de verklaringen van de Certificerend Actuaris en Externe Accountant.

4.3 1e lijn: uitvoerend deel bestuur

SBZ Pensioen heeft een Uitvoerend Bestuurslid Pensioenen en Risicobeheer en een Uitvoerend Bestuurslid Beleggingen en Vermogensbeheer. Dit Uitvoerend Bestuur is verantwoordelijk voor de uitvoering van het beleid ten aanzien van de hun toegewezen aandachtsgebieden. In dit kader bewaken zij de uitbestede werkzaamheden en houden daarmee toezicht op het functioneren van de uitvoeringsorganisaties, en handelen zij operationele zaken af. Daarnaast zijn de Uitvoerende Bestuurders verantwoordelijk voor de beleidsvoorbereiding op deze aandachtsgebieden. Tevens vervullen de Uitvoerende Bestuursleden de eerstelijns-functie voor wat betreft het beheer van de financiële en niet-financiële risico's van het fonds.

Het Uitvoerend Bestuur is actief betrokken bij de commissievergaderingen (zowel bij de opstelling van de agenda en de voorbereiding van stukken als tijdens de vergaderingen).

4.4 2e lijn: Actuariële sleutelfunctie, Sleutelfunctie risicobeheer, Compliance officer, Functionaris Gegevensbescherming / 3e lijn: Sleutelfunctie interne audit

Vanuit het wettelijk kader IORP II heeft het pensioenfonds sleutelfuncties in de 2nd en 3rd line of defence ingericht.
De 2nd line of defence wordt onder meer gevormd door de volgende functies:

- De Sleutelfunctiehouder Risicobeheer zal worden belast met de onafhankelijke advisering over en het toezicht op de uitvoering van het risicobeheerbeleid van het pensioenfonds.
- De Compliance Officer bewaakt dat het pensioenfonds voldoet aan de voor het fonds van toepassing zijnde actuele wet- en regelgeving op het gebied van compliance.
- De Sleutelfunctiehouder Actuarieel ziet onder meer toe op de berekeningen van de technische voorzieningen en premiestelling van een pensioenfonds.
- De Functionaris Gegevensbescherming ziet toe op de vraagstukken die betrekking hebben op privacybescherming en de verwerking van persoonsgegevens.

De Sleutelfunctiehouder Actuarieel, de Compliance Officer en de Functionaris Gegevensbescherming dragen tevens bij aan de doeltreffende toepassing van het risicomanagement.

De 3rd line of defence wordt gevormd door de Sleutelfunctiehouder Interne Audit en is verantwoordelijk voor het aantoonbaar toetsen van de effectiviteit van de 1st line en 2nd line in de uitvoering van het risicomanagement en compliance beleid.

Het pensioenfonds beschikt over de sleutelfuncties Risicobeheer, Interne Audit en Actuarieel met inachtneming van het bepaalde in artikel 143a van de Pensioenwet en artikel 22c van het Besluit FTK. Hierbij maakt het fonds onderscheid tussen de houder en de vervuller(s) van een sleutelfunctie.

Sleutelfunctiehouders zijn eindverantwoordelijk voor de betreffende sleutelfunctie en kunnen (een) Sleutelfunctievervuller(s) aanstellen. De Sleutelfunctiehouder stuurt de Sleutelfunctievervuller aan en

stemt de werkzaamheden van de Sleutelfunctievervuller met hem af. De houder van een sleutelfunctie is geschikt voor het uitoefenen van zijn functie.

De rapportage- en escalatielijnen van de Sleutelfunctiehouders zijn in paragraaf 4.4.4 opgenomen.
In de gevallen genoemd in artikel 143a lid 3 Pensioenwet doet de houder van de betreffende sleutelfunctie een melding aan DNB. Het Bestuur wordt voorafgaand over de melding geïnformeerd.

4.4.1 Sleutelfunctie Risicobeheer

Taken en verantwoordelijkheden sleutelfunctie Risicobeheer
De taken en verantwoordelijkheden van de Sleutelfunctiehouder Risicobeheer zijn uitgebreid vastgelegd in het Reglement Sleutelfunctiehouders. De Sleutelfunctiehouder Risicobeheer beoordeelt, monitort en rapporteert onafhankelijk over (de werking van) het risicobeheersysteem van het pensioenfonds.

Na afloop van ieder kwartaal informeert de Sleutelfunctie Risicobeheer middels de risicorapportage het bestuur over de actuele stand van zaken inzake het risicobeheer van SBZ Pensioen. De risicorapportage omvat de belangrijkste strategische, tactische en operationele ontwikkelingen vanuit risicoperspectief, gerelateerd aan de betreffende risicohouding en risicobereidheid van het bestuur en beoordeeld door de Sleutelfunctie Risicobeheer.

Daarnaast geeft de Sleutelfunctiehouder Risicobeheer via een onafhankelijke risico-opinie zijn/haar mening over de reguliere risicobeoordeling die door het Uitvoerend Bestuur plaatsvindt (middels de risicoparagraaf) bij besluiten, die nieuw beleid of een wijziging van bestaand beleid inhouden.

Inrichting sleutelfunctie Risicobeheer
Voor de Sleutelfunctiehouder Risicobeheer huurt het Bestuur een persoon in op basis van een overeenkomst van opdracht zoals deze ook met Bestuurders wordt gesloten (zogenoemde insourcing). Deze persoon wordt geworven bij de grote aangesloten bedrijven die niet in het Bestuur vertegenwoordigd zijn.
De Sleutelfunctiehouder Risicobeheer maakt een Risicoplan waarin hij risicobeheervervullers uit de diverse organisaties betrekt.

De Sleutelfunctiehouder Risicobeheer wordt ondersteund door de Sleutelfunctievervuller Risicobeheer.
De Sleutelfunctievervuller Risicobeheer:
- ondersteunt de Sleutelfunctiehouder Risicobeheer vanuit de tweede lijn
- geeft input aan de Sleutelfunctiehouder Risicobeheer zodat deze zijn rol goed kan vervullen
- faciliteert de eerste lijn bij hun risicobeheersing, bijvoorbeeld door een risicobeheerraamwerk te leveren en te onderhouden.

Wet Toekomst Pensioenen (WTP)
De Sleutelfunctie Risicobeheer heeft een belangrijke rol in de totstandkoming van een beheerste transitie in het kader van de WTP.
De risicobeheerfunctie draagt vanuit diens controlefunctie bij aan
i) het bevorderen van de risicoalertheid binnen het pensioenfonds en
ii) de advisering over risico's bij deze besluitvorming.
Het is belangrijk dat het bestuur beschikt over advies van de Sleutelfunctie Risicobeheer tijdens transitiebesluitvorming.

Elementen waarbij aantoonbaar advies vanuit de Sleutelfunctie Risicobeheer verwacht wordt, luiden:
Financiële impact
- Zijn de financiële effecten volledig en juist in kaart gebracht?
- Voldoet het besluit aan collectieve actuariële gelijkwaardigheid?

Besluitvormingsproces
- Is er een adequate onderbouwing van de besluitvorming door het bestuur (evenwichtige belangenafweging)?
- Zijn de fondsorganen/-functiesfuncties betrokken in overeenstemming met hun verantwoordelijkheden ten aanzien van de transitie?

Risico's

- Is de beheerste bedrijfsvoering geborgd tijdens de transitie?

Het is de taak van de Sleutelfunctie Risicobeheer er voor te zorgen dat vanuit de eerste lijn de juiste transitierisico's tijdig op de bestuurstafel komen en dat al deze risico's worden doorvertaald naar het transitiepad van SBZ Pensioen.

4.4.2 Sleutelfunctie Actuarieel

Taken en verantwoordelijkheden sleutelfunctie Actuarieel
De taken en verantwoordelijkheden van de Sleutelfunctiehouder Actuarieel zijn uitgebreid vastgelegd in het Reglement Sleutelfunctiehouders. De Sleutelfunctie Actuarieel is belast met de uitvoering van actuariële activiteiten als vastgelegd in artikel 22b van het Besluit financieel toetsingskader pensioenfondsen.

Inrichting sleutelfunctie Actuarieel
Het fonds heeft de Certificerend Actuaris werkzaam bij Willis Towers Watson aangesteld als Sleutelfunctiehouder en -vervuller van de Actuariële functie.

4.4.3 Sleutelfunctie Interne Audit

Taken en verantwoordelijkheden sleutelfunctie Interne Audit
De taken en verantwoordelijkheden van de Sleutelfunctiehouder Interne Audit zijn uitgebreid vastgelegd in het Reglement Sleutelfunctiehouders. De Sleutelfunctiehouder Interne Audit is belast met de activiteiten als vastgelegd in artikel 22a van het Besluit financieel toetsingskader pensioenfondsen.

Inrichting sleutelfunctie Interne Audit
Voor de Sleutelfunctiehouder Interne Audit functie huurt het pensioenfonds een persoon in op basis van een overeenkomst van opdracht zoals deze ook met Bestuurders wordt gesloten (zogenoemde insourcing). Deze persoon wordt bij voorkeur geworven bij de grote aangesloten bedrijven die niet in het Bestuur vertegenwoordigd zijn.
Het onafhankelijke functioneren van de Sleutelfunctiehouder is statutair en contractueel geborgd, mede door de eis dat er geen zakelijke relatie mag zijn met de Bestuursleden.
Het Bestuur kan als Sleutelfunctievervuller een externe partij inschakelen overeenkomstig het uitbestedings- en inkoopbeleid. De onafhankelijke invulling van de werkzaamheden wordt hierbij geborgd.

4.4.4 Rapportage en escalatielijnen Sleutelfunctiehouders

Bij de governance vanuit IORP II hoort ook de vastlegging van de rapportage- en escalatielijnen. De Sleutelfunctiehouder rapporteert periodiek schriftelijk rechtstreeks aan het Bestuur over eventuele materiële bevindingen en aanbevelingen en de opvolgingen ervan op het gebied dat onder zijn verantwoordelijkheid valt.

De Sleutelfunctiehouder Risicobeheer en Actuarieel overleggen voor de dagelijkse aansturing met het Uitvoerend Bestuurslid Pensioenen en Risicobeheer.

De Sleutelfunctiehouder Interne Audit overlegt voor de dagelijkse aansturing met de Onafhankelijk Voorzitter.

De Sleutelfunctievervuller rapporteert onafhankelijk aan de Sleutelfunctiehouder.

Als er naar het oordeel van een Sleutelfunctiehouder niet adequaat wordt gehandeld naar aanleiding van een rapportage, dan kan de betreffende Sleutelfunctiehouder, voor zover de Sleutelfunctiehouder daar nog geen gebruik van heeft gemaakt, gebruik maken van de volgende escalatielijnen:

1. Uitvoerend Bestuur(UB)
2. Onafhankelijk Voorzitter (Vz)
3. Niet-Uitvoerend Bestuur (NUB)

4. De Nederlandsche Bank (DNB)

4.4.5 Compliance Officer

De functie van Compliance Officer is door SBZ Pensioen extern belegd. De Compliance Officer rapporteert aan het Bestuur, zowel voor de dagelijkse gang van zaken, als in het geval zich een bijzondere omstandigheid heeft voorgedaan. Het Bestuur van SBZ Pensioen is en blijft eindverantwoordelijk voor de compliance van SBZ Pensioen. De taken, bevoegdheden en rapportagelijnen zijn nader omschreven in het Compliance Charter en Compliance Program van SBZ Pensioen.

4.4.6 Functionaris Gegevensbescherming

In het kader van een beheerste en integere bedrijfsvoering heeft SBZ Pensioen een Functionaris Gegevensbescherming aangesteld. De Functionaris Gegevensbescherming heeft onder meer de volgende taken, welke zijn vastgelegd in het Charter Functionaris Gegevensbescherming:

- Adviseren over en actualiseren van privacy gerelateerde fondsdocumenten en het privacy statement;
- Monitoren op naleving van de AVG door SBZ Pensioen;
- Monitoren van verwerkers van SBZ Pensioen;
- Informeren en adviseren over verplichtingen ten aanzien van bescherming van persoonsgegevens;
- Adviseren over verwerkersovereenkomsten;
- Adviseren over en beoordelen van het verwerkingsregister;
- Adviseren over en beoordelen van de data protection impact assessment (DPIA);
- Behandelen van vragen en klachten over de verwerking van persoonsgegevens;
- Ondersteunen bij registeren en melden van datalekken bij de Autoriteit Persoonsgegevens (AP);
- Samenwerken met en optreden als contactpersoon voor de AP;
- Onderhouden van contacten met de FG / PO (privacy officer) van verwerkers;
- Rapporteren over privacy aan het Bestuur;
- Volgen van relevante ontwikkelingen in wet- en regelgeving en het Bestuur informeren hierover.

De taken, verantwoordelijkheden en bevoegdheden van de Functionaris Gegevensbescherming zijn opgenomen in het Charter Functionaris Gegevensbescherming.

4.5 Accountant en waarmerkend actuaris

Het geheel van Lines of Defence wordt verder ondersteund door de oordelen van de Certificerend Actuaris en Externe Accountant (4e lijn). SBZ Pensioen verwacht van de Certificerend Actuaris jaarlijks een actuariële rapportage. Van de Externe Accountant wordt verwacht dat jaarlijks de jaarrekening wordt voorzien van een goedkeurende accountantsverklaring. Daarnaast wordt verwacht dat de Externe Accountant een oordeel vormt over de effectiviteit van de governance, de beheersing en het risicomanagement van SBZ Pensioen.

4.6 Toezichthouders

Tenslotte valt SBZ Pensioen onder het toezicht van de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP) en De Nederlandsche Bank (DNB).

De AFM houdt toezicht op de informatieverstrekking door pensioenuitvoerders. De pensioenuitvoerders moeten bepaalde, in de Pensioenwet vastgelegde informatie geven aan de deelnemers, de ex-partners van gescheiden deelnemers, de ex-deelnemers (slapers) en aan de gepensioneerden. Deze informatie moet op tijd, duidelijk, correct en evenwichtig zijn. Informatie op websites of in brochures valt ook onder het toezicht van de AFM. Ook houdt de AFM toezicht op de naleving van de zorgplicht (goed adviseren) bij beschikbare premieregelingen.

De AP houdt onafhankelijk toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. De taken van de AP zijn: toezicht, advisering, voorlichting, informatieverstrekking (via onder meer het Informatie- en Meldpunt Privacy en de website) & verantwoording.

DNB houdt prudentieel en materieel toezicht op de naleving van de pensioenregelgeving door pensioenfondsen. Het prudentieel toezicht is gericht op de financiële soliditeit van pensioenfondsen en het bijdragen aan de financiële stabiliteit van de sector van pensioenfondsen. Materieel toezicht is het toezicht op de naleving van alle normen die geen onderdeel uitmaken van het prudentieel toezicht of het gedragstoezicht waar de AFM mee is belast. Onderdeel van het materieel toezicht betreft het toezicht op de informatiebeveiliging.

Bijlage 1: Risico categorieën

1. Bedrijfsmodel en strategie

1.1. Levensvatbaarheid bedrijfsmodel

1.1.1. Continuïteit uitbesteding:
Het risico dat de continuïteit van (een deel van) de bedrijfsvoering van het pensioenfonds in gevaar komt als gevolg van ontoereikende financiële soliditeit van de tegenpartij, contractbreuk of het beëindigen van de activiteiten door de tegenpartij.

1.1.2. IT Aanpasbaarheid:
Het risico dat IT-omgevingen van pensioenfondsen (en uitvoerders) niet in staat zijn om veranderingen in de bedrijfsvoering als gevolg van interne en externe oorzaken te ondersteunen tegen acceptabele kosten en binnen acceptabele tijd.

1.1.3. Kosten:
Het risico dat actuele of toekomstige (ontwikkeling in) kosten onvoldoende gefinancierd uit dan wel doorvertaald kunnen worden in toekomstige premies, tarieven en/of andere activiteiten.

1.1.4. Productontwikkeling:
Het risico dat het pensioenfonds producten introduceert die:
- niet voldoen aan de eisen en wensen van potentiële klanten
- niet voldoen aan wet- en regelgeving
- onvoldoende rendabel zijn
- ongewenste risico´s (voor het pensioenfonds dan wel voor haar klanten) met zich mee brengen
- bij de introductie onvoldoende ondersteund kunnen worden door de processen, IT en medewerkers van het pensioenfonds.

1.2. Houdbaarheid strategie

1.2.1. Concurrentie:
Het risico dat de concurrentie- en marktpositie van het pensioenfonds wordt beïnvloed als gevolg van activiteiten, acties en/of besluiten van (nieuwe) concurrenten.

1.2.2. Ondernemingsklimaat:
Het risico als gevolg van veranderingen in de omgeving op het gebied van maatschappij of politiek.

1.2.3. Reputatie:
Het risico dat de marktpositie van het pensioenfonds verslechtert als gevolg van negatieve perceptie van het imago van het pensioenfonds door vakbonden, werkgevers, deelnemers, gewezen deelnemers, pensioengerechtigden en/of regelgevende instanties

2. Governance, gedrag, cultuur (GGC) en risicomanagement

2.1. Interne Governance

2.1.1. Aansprakelijkheid:
Het risico dat het pensioenfonds door een rechter aansprakelijk wordt gesteld voor de (materiële of immateriële) schade van derden, onder andere als gevolg van het niet nakomen (dan wel niet in rechte houdbaar zijn) van contractvoorwaarden

2.1.2. Afdwingbaarheid contracten:
Het risico dat verplichtingen van derden jegens het pensioenfonds, of van het pensioenfonds jegens derden, voortvloeiend uit contracten, niet of onvoldoende kunnen worden afgedwongen.

2.1.3. Naleving:
Het risico als gevolg van het niet voldoen van het beleid en/of de bedrijfsvoering van het pensioenfonds aan wet- en regelgeving, alsmede de eigen voorgeschreven beleidskader, processen en procedures van het pensioenfonds.

2.1.4. Personeel:
Het risico voor de doelmatigheid en doeltreffendheid van de uitvoering van de processen op:
- kwalitatieve en/of kwantitatieve personele bezetting
- wervingsproces personeel

2.1.5. Wet- en regelgeving:
Het risico dat de werkwijze van het pensioenfonds (waaronder processen, producten, fiscale constructies) wordt beïnvloed dan wel niet meer houdbaar is als gevolg van veranderingen in de wet- en regelgeving (Europees, (inter)nationaal, toezicht)

2.2. Gedrag en cultuur

2.2.1. Afhankelijkheid:
Het risico dat de invloed van en ontwikkelingen bij vakbonden, werkgevers, deelnemers, gewezen deelnemers en pensioengerechtigden resulteren in conflicterende belangen met het pensioenfonds en/of beïnvloeding van de financiële positie van het pensioenfonds.

2.2.2. Benadeling derden:
Het risico dat reputatieschade en/of claims ontstaan als gevolg van het benadelen van derden door toedoen van het pensioenfonds.

2.2.3. Cybercrime:
Het risico dat schade ontstaat door cybercrime als gevolg van onoplettendheid of onveilig gedrag door eigen personeel, inhuurkrachten of personeel bij uitbestedingspartijen, Cybercrime kan van binnenuit veroorzaakt worden, maar ook door kwaadwillenden van buitenaf.

2.2.4. Externe fraude:
Bij externe fraude gaat het om strafbare, ongewenste en voor het fonds schadelijke handelingen door personen buiten de eigen organisatie.

2.2.5. Fiscale fraude:
Fiscale fraude is fraude met betrekking tot belastingen. Door een onjuist beeld van de werkelijkheid aan de autoriteiten voor te spiegelen wordt ten onrechte minder of geen belasting geheven of wordt een voordeel ten onrechte toegekend.

2.2.6. Integriteit uitbesteding:
Het risico dat de reputatie dan wel de financiële positie van het pensioenfonds wordt geschaad als gevolg van het niet integer zijn van de bedrijfsvoering van de partij waaraan werkzaamheden zijn uitbesteed.

2.2.7. Interne fraude:
Interne fraude betreft strafbare, ongewenste en voor het fonds schadelijke handelingen door personen binnen de eigen organisatie, zijnde de verbonden personen, zoals benoemd in de gedragscode van SBZ Pensioen (bestuur en verantwoordingsorgaan).

2.2.8. Onoorbaar handelen:
Het risico dat de reputatie (en mogelijk ook de financiële positie) van het pensioenfonds wordt beïnvloed als gevolg van het door het pensioenfonds bewust of onbewust faciliteren van of betrokkenheid hebben bij overtredingen.

2.2.9. Voorwetenschap:
Het risico voor het pensioenfonds dat door (werknemers dan wel de leiding van) het pensioenfonds misbruik wordt gemaakt van voorkennis over ontwikkelingen dan wel rechtspersonen. Onder misbruik vallen ook effectentransacties waarbij gebruik wordt gemaakt van verkregen voorkennis.

2.3. Risicomanagement

3. Integriteit

3.1. Witwassen

3.1.1. Witwassen:
Het risico dat schade ontstaat met betrekking tot de reputatie, financiële schade en/of schade door preventief dan wel repressief optreden door de bevoegde autoriteiten als gevolg van (ongewilde) betrokkenheid bij witwassen door klanten, tussenpersonen dan wel eigen personeel.

3.2. Terrorismefinanciering

3.2.1. Terrorismefinanciering:

Het risico dat de reputatie (van het pensioenfonds en de toezichthouder) wordt beïnvloed als gevolg van het verrichten van handelingen door het pensioenfonds met natuurlijke en/of rechtspersonen die betrokken zijn bij (het financieren van) terrorisme of criminaliteit.

3.3. Sancties

3.3.1. Sancties:

Het risico dat de reputatie (van het pensioenfonds en de toezichthouder) wordt beïnvloed als gevolg van het verrichten van handelingen door het pensioenfonds met natuurlijke en/of rechtspersonen waarvoor (inter)nationale sancties gelden.

3.4. Corruptie

3.4.1. Corruptie:

Corruptie is het politieke, sociale of economische verschijnsel waarbij verbonden personen (zoals benoemd in de gedragscode van SBZ Pensioen) ongeoorloofde gunsten verlenen of ontvangen in ruil voor wederdiensten of als vriendendienst. Belangenverstrengeling is een belangrijke oorzaak van corruptie.

3.5. Maatschappelijke onbetamelijkheid

3.5.1. Maatschappelijke onbetamelijkheid:

Het risico dat reputatieschade en/of claims ontstaan als gevolg van het nemen van onvoldoende verantwoordelijkheid ten aanzien van het milieu en de sociale context waarbinnen het pensioenfonds haar kernactiviteiten uitvoert.

4. Prudentiële risico's

4.1. Kredietrisico

4.1.1. Beschikbarepremieregeling en Nettopensioenregeling:

Het risico dat het pensioenkapitaal van deelnemers negatief wordt beïnvloed doordat een debiteur of tegenpartij niet aan zijn verplichtingen voldoet.

4.1.2. Derivaten:

Het kredietrisico bestaat eruit dat een tegenpartij zijn verplichtingen niet na komt.

4.1.3. Geldmarktfondsen:

Het risico dat stukken in geldmarktfondsen onder pari noteren en dat de liquiditeit afneemt.

4.1.4. Herverzekering:

Het risico dat een tegenpartij, waar pensioenaanspraken zijn herverzekerd, niet (meer) aan zijn verplichtingen voldoet.

4.1.5. Hypotheken:

Het risico dat de rente en/of aflossing van hypotheken niet worden betaald.

4.1.6. Obligaties:

Het risico dat obligaties op een voor het pensioenfonds ongunstig moment moeten worden verhandeld.

4.1.7. Transactieafwikkeling:

Het risico dat bij de afwikkeling van een transactie men wel aan zijn eigen verplichtingen voldaan heeft, doch de tegenpartij niet aan diens verplichtingen voldoet (settlementrisico).

4.1.8. Verbruikleen:

Het risico op het onvermogen van een kredietnemer tot teruggave van de bruikleen effecten.

4.1.9. Vorderingen:

Het risico dat aangesloten organisaties de pensioenpremie niet of niet volledig betalen.

4.2. Marktrisico

4.2.1. Beschikbarepremieregeling en Nettopensioenregeling:

Het risico dat het pensioenkapitaal van deelnemers negatief wordt beïnvloed door veranderingen in de waarde van de beleggingen als gevolg van wijzigingen in marktprijzen.

4.2.2. Concentratie en correlatie - Diversificatie en correlatie:
Het risico dat als gevolg van ontoereikende diversificatie binnen de portefeuille een bepaalde ontwikkeling of gebeurtenis een bovengemiddeld effect heeft op de waarde van de portefeuille.

4.2.3. Concentratie en correlatie - Grote posten:
Het risico dat als gevolg van grote posten binnen de portefeuille een bepaalde ontwikkeling of gebeurtenis een bovengemiddeld effect heeft op de waarde van de portefeuille.

4.2.4. Maatschappelijke opvattingen of ontwikkelingen:
Het risico dat beleggingen hun waarde verliezen door veranderende maatschappelijke opvattingen.

4.2.5. Marktliquiditeit - Complexiteit en transparantie:
Het risico dat wordt belegd in producten die qua complexiteit en transparantie niet zijn of worden begrepen door het bestuur.

4.2.6. Marktliquiditeit - Illiquiditeit:
Het risico dat aanwezige activa onvoldoende snel dan wel niet tegen acceptabele prijzen kunnen worden omgezet in liquide middelen.

4.2.7. Marktliquiditeit - OTC:
Het risico op slechte prijsvorming of onvoldoende liquiditeit van OTC (Over The Counter) producten.

4.2.8. Prijsvolatiliteit - Tracking error:
Het risico dat het rendement sterk afwijkt van de waardeontwikkeling van de marktbenchmark.

4.2.9. Prijsvolatiliteit - Volatiliteit:
Het risico van veranderingen in de waarde van (verhandelbare instrumenten binnen) de portefeuille als gevolg van wijzigingen in marktprijzen.

4.2.10. Prijsvolatiliteit - Voorspelbaarheid:
Het risico op down fall als gevolg van muteren van de beleggingsportefeuille op ongunstige handelsmomenten.

4.3. Renterisico

4.3.1. Beschikbarepremieregeling en Nettopensioenregeling:
Het risico dat het pensioenkapitaal van deelnemers negatief wordt beïnvloed doordat rentefluctuaties - als gevolg van ontoereikende afstemming tussen rentegevoelige activa en het benodigde kapitaal op pensioendatum - leiden tot ongewenste effecten.

4.3.2. Inflatie:
Het risico dat het pensioenfonds onvoldoende in staat is om (toenemende) verplichtingen als gevolg van (verwachte aanpassing aan) inflatie te financieren zonder belanghebbenden te benadelen.

4.3.3. Rente - Gevoeligheid yieldcurve:
Het risico dat rentefluctuaties - als gevolg van veranderingen in absolute hoogte en vorm van yieldcurven - leiden tot ongewenste effecten op balans en resultaat.

4.3.4. Rente - Looptijdverschil:
Het risico dat rentefluctuaties - als gevolg van ontoereikende afstemming tussen rentegevoelige activa en passiva (inclusief off-balanceposten) op het gebied van renteloopt ijden - leiden tot ongewenste effecten op balans en resultaat.

4.3.5. Rente - Voorspelbaarheid renteontwikkeling:
Het risico dat de werkelijke renteontwikkeling in afwijking op het bij het vaststellen van het beleid veronderstelde renteontwikkeling leidt tot ongewenste effecten op balans en resultaat.

4.3.6. Valuta:
Het risico als gevolg van onvoldoende afstemming tussen activa en passiva, dan wel inkomsten en uitgaven op het gebied van vreemde valuta

4.4. Operationeel risico

4.4.1. (Pre)acceptatie/transactie:
Het risico van onvoldoende doelmatige en/of onvoldoende doeltreffende processen op het gebied van het aangaan van nieuwe betrekkingen (klantacceptatie, prijsbepaling en onderhandeling) met (nieuwe) klanten of tegenpartijen met betrekking tot de kernactiviteiten van het pensioenfonds.

4.4.2. Informatie:
Het risico dat de informatievoorziening niet juist, tijdig en volledig is, waardoor het adequaat sturen en beheersen van de betreffende activiteit ter ondersteuning van adequate managementbeslissingen niet mogelijk is.

4.4.3. IT Beschikbaarheid:
Het binnen een redelijke tijdstermijn kunnen raadplegen of wijzigen van gegevens wanneer dit bij het uitvoeren van werkzaamheden nodig is, ofwel het draaiend houden van bestaande processen en het herstellen van verstoringen, waarbij de negatieve gevolgen van incidenten (uitval, beveiligingslekken) worden beperkt.

4.4.4. IT Integriteit:
Het in overeenstemming zijn van gegevens met het afgebeelde deel van de realiteit en dat niets ten onrechte is achtergehouden of verdwenen, i.c. de aspecten juistheid, volledigheid en tijdigheid, ofwel het opleveren van juiste, tijdige en volledige informatie aan alle relevante belanghebbenden.

4.4.5. IT Vertrouwelijkheid:
De beperking van de bevoegdheid en mogelijkheid tot uitlezen, kopiëren of kennisnemen van informatie en van andere systeemcomponenten tot een gedefinieerde groep van gerechtigden, ofwel het waarborgen dat de juiste mensen toegang hebben tot de juiste informatie en anderen niet.

4.4.6. Kwaliteit uitbesteding:
Het risico dat de door de externe partij geleverde kwaliteit van de werkzaamheden niet in overeenstemming is met het door het pensioenfonds gewenste dan wel aan belanghebbenden toegezegde kwaliteitsniveau.

4.4.7. Uitkering/betaling/settlement:
Het risico dat de doelmatigheid en doeltreffendheid van de uitvoering van het betalingsproces, settlement en/of clearingproces wordt beïnvloed.

4.4.8. Verwerking:
Het risico dat de doelmatigheid en doeltreffendheid van het verwerkingsproces wordt beïnvloed als gevolg van:
- inadequaat administreren van transacties en data;
- inadequaat bepalen en doorberekenen van premies en andere tarieven;
- inadequate klantenservice.

4.4.9. Information Security Management System (ISMS):
Het risico dat de IT-risicomanagementcyclus van het fonds niet goed functioneert, waardoor identificatie, evaluatie, beheersing en monitoring van IT-risico's niet voldoende plaats vindt, met als gevolg operationele verstoringen, financiële schade, reputatieschade en/of juridische / compliance risico's.

4.5. Liquiditeitsrisico

4.5.1. Liquiditeit:
Het risico dat liquiditeitstekorten optreden als gevolg van het onvoldoende op elkaar afgestemd zijn van de timing en de omvang van inkomende en uitgaande kasstromen.

4.6. Verzekeringstechnisch risico

4.6.1. Arbeidsongeschiktheid:
Het risico dat verliezen optreden als gevolg van verschillen tussen:
- de werkelijke en de veronderstelde arbeidsongeschiktheid (inclusief revalidatie);
- de werkelijke en de veronderstelde ontwikkeling in de verwachtingen inzake arbeidsongeschiktheid (inclusief revalidatie).

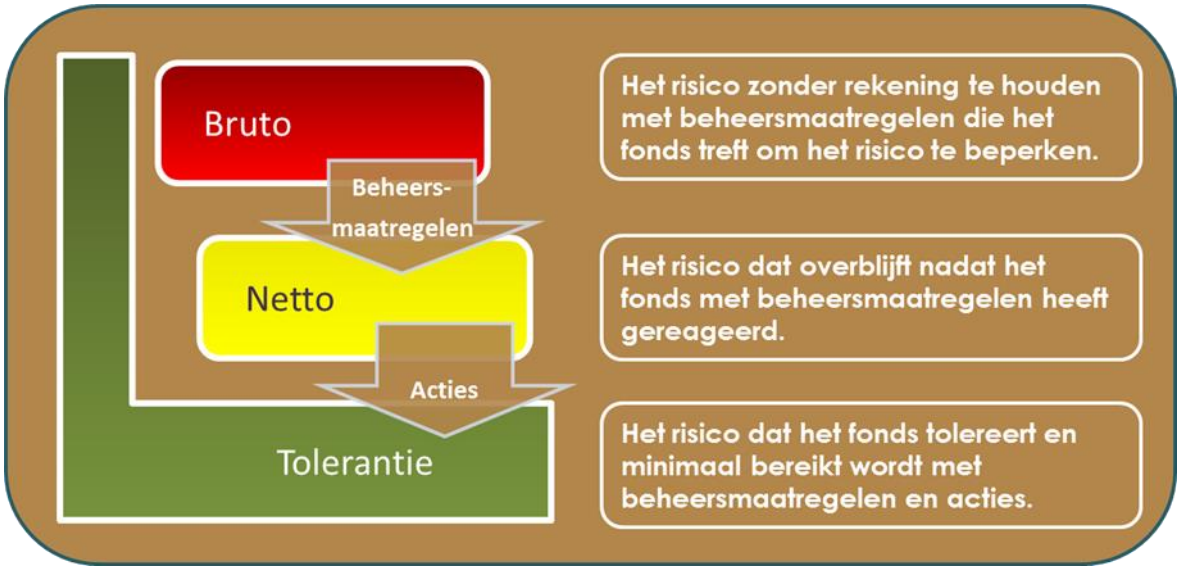
4.6.2. Sterfte:
Het risico dat verliezen optreden als gevolg van verschillen tussen
- de werkelijke en de veronderstelde sterfte;

- de werkelijke en de veronderstelde ontwikkeling in de sterfteverwachtingen.

5. Kapitaal
5.1. Kapitaalpositie

Bijlage 2: Risicoclassificatie

De geïdentificeerde risico's worden kwalitatief beoordeeld op basis van de waarschijnlijkheid van het optreden van het risico en de impact daarvan op het behalen van de doelstellingen. Hierbij wordt een onderscheid gemaakt tussen het bruto risico, het netto risico en de risicotolerantie. De volgende figuur geeft dit kort weer.



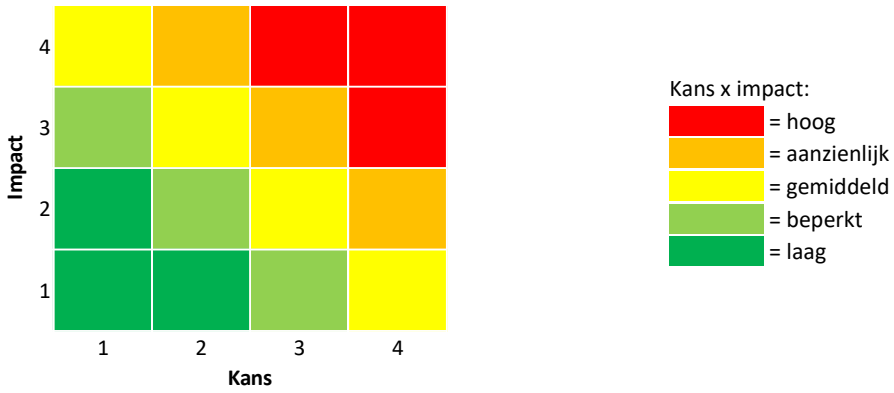
Het bruto risico is het risico zonder rekening te houden met eventuele beheersmaatregelen die SBZ Pensioen treft om de waarschijnlijkheid en/of impact te beperken. Het bruto risico is afhankelijk van de context waarbinnen SBZ Pensioen opereert en diens doelstellingen.

Ten aanzien van het bruto risico zijn vanuit de risicotolerantie vier mogelijke reacties te onderscheiden:
- het risico accepteren;
- het risico reduceren door het nemen van aanvullende beheersmaatregelen;
- het risico vermijden door de activiteiten die geraakt worden door het risico te staken;
- het risico overdragen door de activiteiten die door het risico geraakt worden (deels) uit te besteden.

Het netto risico is het risico dat overblijft na implementatie van beheersingsmaatregelen op de bruto risico's. Indien het netto risico vanuit de risicotolerantie (nog) niet acceptabel is, definieert SBZ Pensioen aanvullende acties om tot de risicotolerantie te komen.

Dit leidt tot gemeenschappelijk inzicht in de risico's die SBZ Pensioen loopt, de beheersmaatregelen die zijn genomen en de beheersmaatregelen die nog moeten worden genomen of gewenst zijn.

De inschattingen van het bruto en netto risico en de risicotolerantie worden geplot in een risicomatrix (duiding van de kans en impactniveaus zijn hieronder nader uitgewerkt):



Financiële risico's

Bij de risicokwantificatie van de financiële risico's wordt de volgende duiding als referentieschaal gebruikt:

Niveau	Kans	Impact
4. Hoog	*Voor bruto en tolerantie:* Treedt op het komend jaar. *Voor netto:* Heeft zich het afgelopen jaar voorgedaan.	Mogelijke daling dekkingsgraad in enig jaar bedraagt meer dan 13%.[5] of Beleidsdekkingsgraad daalt onder 100% (uitgaande van een solide financiële positie van het fonds).
3. Aanzienlijk	*Voor bruto en tolerantie:* Heeft de potentie om op te treden binnen het komend jaar. *Voor netto:* Heeft zich voorgedaan de afgelopen 2 jaar.	Mogelijke daling dekkingsgraad in enig jaar bedraagt 6,5% tot 13%. of Beleidsdekkingsgraad daalt onder 105% (uitgaande van een solide financiële positie van het fonds).
2. Beperkt	*Voor bruto en tolerantie:* Doet zich mogelijk voor binnen 3 jaar. *Voor netto:* Heeft zich voorgedaan de afgelopen 5 jaar.	Mogelijke daling dekkingsgraad in enig jaar bedraagt 0% tot 6,5%. of Beleidsdekkingsgraad daalt onder 110% (uitgaande van een solide financiële positie van het fonds).
1. Laag	*Voor bruto en tolerantie:* Onwaarschijnlijk dat het zich voordoet de komende 5 jaar. *Voor netto:* Heeft zich niet eerder voorgedaan binnen het fonds.	Dekkingsgraad wordt niet negatief beïnvloed.

[5] De genoemde 13% is ontleend aan het verschil tussen het VEV ad 117% (afgerond) en het MVEV ad 104% (afgerond). De hoogte van het VEV is gericht op de wettelijke zekerheidsmaat van 97,5%, dat wil zeggen dat in de evenwichtssituatie de kans dat het pensioenfonds binnen een periode van één jaar over minder waarden beschikt dan de technische voorzieningen, kleiner is dan 2,5%.

Niet-financiële risico's
Bij de risicokwantificatie van de niet financiële risico's wordt de volgende duiding als referentieschaal gebruikt:

Niveau	Kans	Impact
4. Hoog	*Voor bruto en tolerantie:* Treedt op het komend jaar. *Voor netto:* Heeft zich het afgelopen jaar voorgedaan.	Risico op negatieve publiciteit richting pensioensector. Structureel negatieve reacties vanuit DNB/AFM. Het niveau van dienstverlening van het fonds wordt beïnvloed, met als gevolg een grote daling van de tevredenheid van deelnemers. Erg moeilijk te herstellen (herstelkosten zijn hoger dan 10 bp[6] van het totale vermogen).
3. Aanzienlijk	*Voor bruto en tolerantie:* Heeft de potentie om op te treden binnen het komend jaar. *Voor netto:* Heeft zich voorgedaan de afgelopen 2 jaar.	Risico op negatieve publiciteit richting pensioensector. Negatieve reacties vanuit DNB/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 (herstelkosten zijn lager dan 10 bp van het totale vermogen).
2. Beperkt	*Voor bruto en tolerantie:* Doet zich mogelijk voor binnen 3 jaar. *Voor netto:* Heeft zich voorgedaan de afgelopen 5 jaar.	Risico op interne negatieve / 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 (herstelkosten zijn lager dan 1 bp van het totale vermogen).
1. Laag	*Voor bruto en tolerantie:* Onwaarschijnlijk dat het zich voordoet de komende 5 jaar. *Voor netto:* Heeft zich niet eerder voorgedaan binnen het fonds.	Risico op interne negatieve / kritische berichtgeving (incl. uitvoerders). Het niveau van dienstverlening van het fonds wordt beïnvloed, maar geen gevolgen voor de tevredenheid van deelnemers. Makkelijk te herstellen (herstelkosten zijn lager dan 0,1 bp van het totale vermogen).

[6] Zijnde circa 20% van de totale kosten vermogensbeheer.

In aanvulling op de risico classificatie in Bijlage 2 is voor de classificaties beschikbaarheid, vertrouwelijkheid en aanpasbaarheid van systemen en data het volgende van toepassing:

IT-beschikbaarheid
Afhankelijk van de impact is per proces een eis geformuleerd voor de maximaal geaccepteerde ‘downtime’ met het oog op herstel van kritieke systemen (RTO) en het maximaal geaccepteerde dataverlies (RPO).

IT-integriteit
n.v.t., geen toevoegingen

IT-vertrouwelijkheid
De classificatie van persoonsgegevens worden tenminste opgenomen in de categorie ‘Aanzienlijk’. Bijzondere persoonsgegevens vallen in de categorie ‘Hoog’.

Als uitgangspunt geldt dat voor gegevens in transport en in opslag geclassificeerd op niveau 3 en 4 encryptie een verplichte maatregel is indien een gerelateerd risico buiten de risicotolerantie van SBZ Pensioen valt. De classificatie van gegevens vindt plaats als onderdeel van de IT-risicoanalyse.

IT-aanpasbaarheid
Voor aanpasbaarheid op IT-systemen geldt een afwijkende risicoclassificatie:
4 – essentieel: zeer grote mate van aanpasbaarheid is van kritisch belang. De applicatie ondersteunt een of meerdere bedrijfskritieke processen die nu of in de nabije toekomst onderhevig (zullen) zijn aan complexe wijzigingen als gevolg van interne of externe ontwikkelingen.
3 – noodzakelijk: Een grote mate van aanpasbaarheid is van belang. De applicatie ondersteunt een of meerdere processen die nu of waarschijnlijk in de nabije toekomst onderhevig zijn aan complexe(re) wijzigingen als gevolg van interne of externe ontwikkelingen.
2 – belangrijk: Een zekere mate van aanpasbaarheid is belangrijk. De applicatie ondersteunt een of meerdere processen die waarschijnlijk in de nabije toekomst onderhevig zijn aan (eenvoudige) wijzigingen als gevolg van interne of externe ontwikkelingen.
1 – niet nodig: Aanpasbaarheid is niet nodig. De applicatie (of het systeem) ondersteunt een proces dat niet of nauwelijks aan verandering onderhevig is. De applicatie is eenvoudig te vervangen door vergelijkbare applicaties. Veranderingen als gevolg van interne en externe oorzaken zijn minimaal.