

Geachte bestuurders,

Sinds 13 januari 2019 moeten pensioenfondsen en premiepensioeninstellingen (PPI's) minimaal eens in de drie jaar een eigen risicobeoordeling (ERB) uitvoeren en de resultaten daarvan met DNB delen. De eerste cyclus van drie jaar is afgelopen. Op basis van een representatieve selectie heeft DNB nu beoordeeld of de ERB's voldoen aan alle wettelijke vereisten en hoe strategische risico's, duurzaamheid en datakwaliteit in de ERB zijn geadresseerd.

We zien dat de sector serieus werk maakt van de ERB's. De instellingen gebruiken de ERB als instrument om kritisch te bekijken in hoeverre strategische doelen onder druk staan en of de instelling de beheersing om deze doelen te halen op orde heeft.

De sector heeft een goede start gemaakt en tegelijk zijn er nog mogelijkheden tot verbetering. In deze sectorbrief leest u de uitkomsten van de beoordeling zodat u als instelling zelf kunt bepalen welke punten u meeneemt bij het opstellen van een volgende ERB.

Geconstateerde verbeterpunten

1	Zelfstandige leesbaarheid ERB verbeteren
2	Triggers voor tussentijdse ERB benoemen
3	Rollen in besluitvormingsproces ERB vastleggen en interne organen betrekken
4	Separaat oordeel sleutelfunctiehouder(s) opnemen
5	Zowel bruto als netto risico's beoordelen
6	Inhoudelijk oordeel over doelmatigheid risicobeheer verbeteren
7	Verantwoording van de volgende thema's in de ERB verbeteren
	1. Strategische risico's opnemen in risicomangementcyclus met oordeel sleutelfunctiehouder Risicobeheer
	2. ESG risicobeheer aansluiten op good practice ESG
	3. Aandacht in de ERB vergroten voor het risico datakwaliteit waaronder juistheid en volledigheid van relevante pensioengegevens

ERB op tijd vastgesteld en ingediend

Alle pensioeninstellingen hebben tijdig een ERB vastgesteld en nagenoeg alle instellingen hebben deze binnen de wettelijke termijn van 14 dagen na vaststelling aangeleverd bij DNB.

Instellingen hebben zichtbaar veel tijd en aandacht besteed aan het op- en vaststellen van de ERB. De analyse toont aan dat het overgrote deel van de ERB's goed gestructureerd is, vaak conform de handreiking van de Pensioenfederatie, en dat die specifiek de situatie en context van de instelling beschrijft en op veel van de relevante onderwerpen en ontwikkelingen verdieping aanbrengt.

Verbeterpunt 1: Zelfstandige leesbaarheid ERB verbeteren

De zelfstandige leesbaarheid van de ERB's is een punt van aandacht. De ERB is een op zichzelf staand document, waarin alle essentiële informatie zelfstandig leesbaar is uitgeschreven¹. Frequent worden aan de ERB ten grondslag liggende documenten aangehaald. Het is belangrijk dat de instelling de meest relevante onderdelen uit deze documenten ook (kort) terug laat komen in de ERB-uitwerking. Refereren naar onderliggende documenten zonder de essentie te vatten in de ERB is derhalve niet toereikend. Een concrete weergave van kenmerken, keuzes en risico's zorgt dat ook de ontvanger zonder (diepgaand) begrip van de onderliggende documenten de ERB kan lezen, bevatten en beoordelen. Het gebruik van tabellen en grafieken is een manier om inzicht te geven, bijvoorbeeld in de belangrijkste kengetallen voor de financiële opzet.

¹ Zie voor deze punten de [Factsheet Eigen Risico Beoordeling: inhoud en proces](#).

Verbeterpunt 2: Triggers voor tussentijdse ERB benoemen

In een groot aantal ERB's wordt benoemd dat er 'triggers' kunnen zijn die tot een tussentijdse ERB leiden, maar voorbeelden van de triggers die de instelling heeft vastgesteld ontbreken regelmatig. Het overgrote deel van de beoordeelde ERB's vermeldt dat de bij DNB ingediende ERB een 'reguliere / driejaarlijkse' ERB betreft. In dat kader wordt opgemerkt dat bij materiële beleidswijzigingen een tussentijdse ERB nodig kan zijn. In sommige ERB's zijn wel voorbeelden opgenomen van zogenoemde triggers. Een aantal voorbeelden van triggers die we zijn tegengekomen: wijzigingen in de pensioenregeling, wijzigingen in pensioenwetgeving, escalatie van issues uit interne beheersing, wisseling van pensioenuitvoeringsorganisatie, wijzigingen in strategie of eigendomsverhouding bij belangrijke partners.

We zien daarnaast dat sommige instellingen kiezen om een reguliere ERB een plek te geven in bestuurlijke kalender door aansluiting te zoeken bij de ALM cyclus. Deze cyclus is vaak ook driejaarlijks en kan nieuwe strategische inzichten geven die aanleiding zijn de ERB opnieuw uit te voeren. Hiermee wordt de ERB opgenomen in de strategische cyclus van de instelling.

Verbeterpunt 3: Rollen in besluitvormingsproces ERB vastleggen en interne organen betrekken

Nagenoeg alle instellingen hebben een duidelijke beschrijving opgenomen waaruit blijkt dat de ERB integraal onderdeel uitmaakt van de (risico)management processen. DNB ziet ruimte voor verbetering door te beschrijven hoe de ERB is geborgd in de besluitvormingsprocessen van de instelling.

De analyse heeft aangetoond dat de betrokkenheid van de interne organen van de instellingen verschilt als het gaat om de totstandkoming en goedkeuring van de ERB. Er bestaat een grote variëteit in de wijze waarop, en mate waarin, functies en organen betrokken zijn geweest bij de totstandkoming van de ERB. In een aantal gevallen zijn alleen het bestuur en het bestuurs- of pensioenbureau van de instelling genoemd in de ERB. De betrokkenheid van bijvoorbeeld de sleutelfunctiehouder(s), bestuurlijke commissies en toezichhoudende organen bij de ERB kan dan niet zomaar worden vastgesteld. In sommige gevallen kan nog wel betrokkenheid van bepaalde groepen worden vastgesteld vanuit de ERB-governance, bijvoorbeeld als uit een plan van aanpak of een tijdslijn blijkt dat er een brede en doorlopende betrokkenheid is, bij een of meerdere van de volgende processen

- het vaststellen van de scope van de ERB
- het selecteren van een beoordelingsaanpak
- het doorlopen van de beoordeling
- het afstemmen van de uitkomsten van de ERB

Een aantal instellingen heeft gekozen om de betrokken personen en organen (binnen én buiten de instelling) inzichtelijk te maken met een RA(S)CI-model waarin de rollen en verantwoordelijkheden staan beschreven.

Verbeterpunt 4: Separaat oordeel sleutelfunctiehouder(s) opnemen

In de meeste beoordeelde ERB's is niet vastgelegd of één of meerdere sleutelfunctiehouders de ERB-uitkomsten bekrachtigd hebben en hoe zij het doorlopen ERB-proces beoordelen. Iedere instelling heeft meerdere sleutelfunctiehouders (hierna: SFH's): pensioenfondsen hebben een SFH risicobeheer, een SFH interne audit en een SFH actuariael en PPI's hebben een SFH risicobeheer en een SFH interne audit. In de [Q&A Geschiktheidseisen sleutelfunctiehouder risicobeheer functie](#) is beschreven dat in ieder geval de SFH risicobeheer een actieve rol vervult bij de totstandkoming en vaststelling van de ERB. Die actieve rol is echter regelmatig niet of onvoldoende zichtbaar in de ERB. We zien ook ERB's waarin alle SFH's wel actief betrokken zijn bij de totstandkoming van de ERB's. Dit is zichtbaar gemaakt doordat de drie SFH's ieder vanuit de eigen rol en verantwoordelijkheid een separate opinie bij de ERB hebben opgesteld.

Verbeterpunt 5: Zowel bruto als netto risico's beoordelen

Bij het beoordelen van de risico's wordt in veel beoordeelde ERB's de bruto-netto methodiek toegepast, maar sommige ERB's geven alleen de netto risicoscore, waardoor niet is vast te stellen hoe de instelling aankijkt tegen het bruto risico en (de effectiviteit van) de beheersmaatregelen. Met de bruto-netto methodiek is voor de belangrijkste risico's duidelijk zichtbaar welke beheersmaatregelen er zijn voor de risico's en de impact die dat risico kan hebben op de instelling. Ook wordt hiermee een duidelijke koppeling gelegd met de risicobereidheid van de instelling.

Bij een aantal instellingen ziet DNB daarnaast een starttabel in de ERB waarin per risico of risicocategorie staat uitgewerkt:

- wat de bruto risico-inschatting is van de kans en impact van dit risico,
- een overzicht met getroffen (beheers)maatregelen om de kans en/of impact van dit risico te mitigeren,
- een beoordeling of deze beheersmaatregelen het risico mitigeren binnen de risicobereidheid, en
- als dit (nog) niet het geval is, welke (SMART-beschreven) aanvullende maatregelen en/of acties genomen worden of kunnen worden om dit alsnog te realiseren.

Verbeterpunt 6: Inhoudelijk oordeel over doelmatigheid risicobeheer verbeteren

De doelmatigheid van het risicobeheer wordt in alle ERB's beoordeeld. Wel constateert DNB dat de vastlegging van de wijze waarop het bestuur tot haar oordeel over de doelmatigheid is gekomen sterk verschilt. Een beperkt aantal ERB's brengt veel diepte aan in een beschrijving a) hoe de beoordeling heeft plaatsgevonden en b) wie bij deze beoordeling betrokken is geweest, om vervolgens c) een uitgewerkt oordeel te geven rond de doelmatigheid, waarbij concrete vervolgstappen en acties worden benoemd om de doelmatigheid van het risicobeheer verder te versterken. Daarentegen bevat een groot aantal ERB's uitsluitend de vermelding van 'het oordeel' over de doelmatigheid van het risicobeheer.

De doelmatigheid van risicobeheer is daarnaast vaak niet volledig beschreven. We hebben weinig gezien dat een ERB concreet beschrijft wat het bestuur en de interne toezichthouders verstaan onder 'doelmatig', waardoor vaak ook niet duidelijk is hoe die doelmatigheid wordt beoordeeld en onderbouwd.

Sommige instellingen halen voorafgaand aan de beoordeling van de doelmatigheid individuele (denk)beelden bij de individuele bestuurders op en bespreken deze uitkomsten in een geconsolideerde vorm binnen het bestuur, om zo te komen tot een breed gedragen oordeel van deze doelmatigheid. Meestal wordt ook gekozen om dit bestuurlijke oordeel tevens te bespreken met het intern toezicht van de instelling, zoals het Verantwoordingsorgaan en/of de Raad van Toezicht.

Ook wanneer verbeterpunten door het bestuur zijn vastgesteld om de doelmatigheid te verhogen, is het mogelijk een positief oordeel te hebben over de doelmatigheid. Het hebben van verbeterpunten leidt niet automatisch tot het oordeel dat de doelmatigheid onvoldoende is. Het goed vastleggen van het oordeel over de doelmatigheid zelf én de onderbouwing van dat oordeel ziet DNB in een aantal ERB's terugkomen.

Verbeterpunt 7: Verantwoording van de volgende thema's in de ERB verbeteren

DNB heeft tot slot in de analyse op drie thema's een inhoudelijke verdieping uitgevoerd. De uitkomsten worden per thema hieronder weergegeven.

7.1 Strategische risico's opnemen in risicomanagementcyclus met oordeel sleutelfunctiehouder Risicobeheer

De analyse toont aan dat de meeste ERB's een toereikende set aan strategische risico's hebben beoordeeld. Het identificeren van de belangrijkste (strategische) risico's die missie, visie en doelstellingen van een instelling in gevaar kunnen brengen is een belangrijke doelstelling van de ERB. DNB constateert dat de instellingen hier invulling aan geven. In ongeveer de helft van de ERB's is voor de identificatie van strategische risico's gebruik gemaakt van scenario's, waardoor de strategische

risico's meer integraal worden behandeld. In die gevallen zijn de risico's beoordeeld in samenhang met de missie, visie en de strategische doelstellingen van de instelling.

Bij meerdere instellingen ziet DNB dat strategische risico's in de kwartaalrapportage worden meegenomen en voorzien van een (risico)opinie vanuit de sleutelfunctiehouder risicomanagement, waarbij wordt ingezoomd op de eventueel bestaande afwijkingen van de inschatting van strategische risico's als onderdeel van de ERB. Niet alle beoordeelde ERB's bieden echter transparantie in de wijze waarop over de strategische risico's wordt gerapporteerd (inclusief periodiciteit waarmee) en de rol van de sleutelfunctiehouder risicomanagement hierin.

In veel ERB's wordt met het uitvoeren van de ERB geconstateerd dat er nieuwe risico's aan het strategisch risico-universum dienen te worden toegevoegd of meer geëxpliciteerd opgenomen en aanvullende (beheers)maatregelen moeten worden geïmplementeerd. In een aantal gevallen zaten deze risico's al in het risico-universum, maar was tot dat moment de inschatting dat die risico's geen directe impact zouden hebben op het realiseren van de instellingsdoelstellingen. Bij deze instellingen ging het de facto dus niet om volledig nieuwe risico's, maar is nieuw dat ze in de ingediende ERB als strategisch risico zijn geïdentificeerd. Veel genoemde voorbeelden van nieuwe of zwaarderwegende strategische risico's, zijn risico's op het gebied van ESG, cybersecurity en de Wet Toekomst Pensioenen, maar ook bestuurlijke / governance gerelateerde risico's en risico's met betrekking tot ontwikkelingen bij uitbestedingsrelaties.

Uit de analyse van de beoordeelde ERB's komt het beeld naar voren dat de uitkomsten van de systematische integriteitsrisicoanalyse (SIRA) in het merendeel van de ERB's niet of in beperkte mate worden meegenomen. Zo wordt de SIRA slechts in circa de helft van de beoordeelde ERB's genoemd als referentiedocument. Het expliciet en met gewenste diepgang voor de ERB benoemen van de uitkomsten van de SIRA en de potentiële impact op de strategische risico's van de instelling gebeurt slechts in enkele gevallen.

7.2 ESG-risicobeheer aansluiten op good practice ESG

Wetgeving voor pensioenfondsen en PPI's² benoemen ESG (Environment, Social, Governance) als een risico dat, indien van toepassing op een pensioeninstelling, in de ERB dient te worden beoordeeld.

DNB constateert dat ESG in nagenoeg iedere beoordeelde ERB als risicocategorie terug komt. ESG risico's kunnen pensioeninstellingen op diverse manieren aangrijpen zoals op financieel, reputationeel, compliance en operationeel vlak. Bij de beoordeling van de ERB's zien we dat het thema ESG regelmatig genoemd wordt in het kader van maatschappelijke verantwoordelijkheid. ESG wordt hierbij in veel gevallen beschouwd vanuit het 'ESG- of MVO-beleid' en 'Investment Beliefs'. De concrete koppeling vanuit dit beleid met de bijbehorende risico's ontbreekt veelal.

De scope en diepgang waarbinnen de ESG-risico's worden beschouwd, bieden veel ruimte tot verbetering. Uit de analyse blijkt dat de scope van de ESG-beschouwing in de meeste gevallen beperkt is tot 'Klimaatrisico', waardoor uitwerking van andere ESG-elementen (waaronder sociale risico's, gebruik van hulpbronnen en governance risico's) ontbreekt.

Instellingen die concluderen dat ESG-risico's slechts een beperkte impact hebben op de strategische doelen vermelden en onderbouwen dit zelden in de ERB.

DNB brengt in 2022 een good practice uit op het gebied van het beheer van ESG-risico's. Deze good practice kan de sector gebruiken om op een goede manier invulling te geven aan en het verankeren van het risicobeheer van ESG-risico's.

² Artikel 18b, tweede lid, sub h van het Besluit FTK (voor pensioenfondsen) en artikel 26.02, tweede lid, sub a, juncto artikel 26, tweede lid, sub d van het Besluit prudentiële regels Wft (voor PPI's)

7.3 Aandacht in de ERB vergroten voor het risico datakwaliteit waaronder juistheid en volledigheid van relevante pensioengegevens

DNB heeft de afgelopen jaren richting de sector het belang van datakwaliteit benadrukt. Met de komst van de Wet Toekomst Pensioen neemt het belang van juiste, volledige en reproduceerbare data op het transitie-moment verder toe. DNB ziet datakwaliteit als thema / risico beperkt terugkomen in de ERB.

Datakwaliteit is als thema opgenomen in een beperkt aantal ERB's, waarbij opvalt dat datakwaliteit hoofdzakelijk wordt gewogen vanuit een cyber- en privacy-perspectief. Er wordt beperkt - of in bovengemiddeld aantal gevallen niet - ingezoomd op de juistheid en volledigheid van de (pensioenadministratie) data en de tijdigheid, bijvoorbeeld van het verwerken van wijzigingen. Datakwaliteit wordt in veel gevallen opgehangen aan risicocategorieën waarbij een relatie is met beschikbaarheid en veiligheid van data. Dit is gezien de ontwikkelingen met betrekking tot cyber criminaliteit een goede constatering, maar het is slechts één kant van de medaille.

DNB ziet dat weinig aandacht wordt besteed aan de wijze waarop de risico's met betrekking tot juiste, volledige en tijdige verwerking van data in de pensioenadministratie worden beheerst.

Door de nieuwe Wet Toekomst Pensioen werkt de sector naar een waarheidsmoment waarbij zij verantwoording gaat afleggen aan haar deelnemers over de data. Indien gekozen wordt voor invaren, hebben instellingen één transitie-moment om het invaren goed uit te voeren. Om verantwoording te kunnen afleggen is het nodig dat de juistheid en volledigheid van de data worden vastgesteld. De instelling zal hiertoe een risicotolerantie moeten vaststellen, de datakwaliteit moeten analyseren, meten en corrigeren en nagaan of de datakwaliteit op het transitie-moment 'goed genoeg' is. Met andere woorden, binnen de risicotolerantie van de instelling blijft.

De aandacht voor het risico op onjuiste en onvolledige data in de ERB's vinden wij veelal nog onvoldoende. Nu ontbreekt vaak structurele aandacht voor de inhoudelijke controles op data van pensioengegevens (data-controles) om de juistheid en volledigheid van aanspraken te valideren en hierover structurele (bestuurlijke) rapportages te ontvangen op de uitkomsten en follow-up hiervan. Zie voor beheersing van datakwaliteit de [Good Practice Robuuste Pensioenadministratie](#).