DeNederlandscheBank
EUROSYSTEEM

[Naam pensioenfonds]
T.a.v. het bestuur
[Postadres]
[Postcode] [Plaats]

De Nederlandsche Bank N.V.
Expertisecentrum Operationele & IT-risico's

Postbus 98
1000 AB Amsterdam
+31 20 524 91 11
www.dnb.nl

Handelsregister 3300 3396

Onderwerp
Terugkoppeling onderzoek 'inventarisatie uitbesteding'

Datum
29 augustus 2018

Uw kenmerk

Ons kenmerk
T039-919612099-216

Behandeld door
Talsma, I.J. (Ingrid)
Wortman, R. (Rebecca)

Bijlagen
1

Geachte bestuur,

In 2017 heeft DNB een onderzoek door middel van een self- assessment uitgevoerd naar uitbesteding en de beheersing van het uitbestedingsrisico. Aanleiding van dit onderzoek was de verwachte toename in de aard van uitbestede bedrijfsactiviteiten, waaronder cloud uitbestedingen. Aandacht hiervoor is belangrijk, omdat de verwachting is dat de risico's op dit vlak in de komende jaren toenemen. In deze brief leest u meer over de uitkomsten van het onderzoek en wat DNB van u verwacht.

Uitkomsten onderzoek

Pensioenfondsen besteden veel uit waarbij ketens van uitbestedingen langer en complexer worden. Dit stelt hoge eisen aan de besturing van uitbestedingen en de beheersing van risico's die hiermee samenhangen. De resultaten van dit onderzoek laten zien dat er ruimte voor verbetering is bij de beheersing van de (onder-)uitbestedingsrisico's. Bij een (groot) aantal instellingen blijken de belangrijkste bevindingen uit het onderzoek:

- Uitbestedingen worden niet structureel centraal geregistreerd.
- Het interne beleid voldoet niet bij alle pensioenfondsen aan de wettelijke vereisten
- Bestuurders ontvangen niet op reguliere basis managementinformatie over uitbestedingen, daaronder begrepen ook onderuitbestedingen
- Evaluatie van dienstverleners schiet tekort in zowel frequentie als kwaliteit
- Activiteiten uitgevoerd door dienstverleners worden niet structureel meegenomen in Business Continuity Management
- Er zijn niet altijd voldoende beheersmaatregelen om de toegang van dienstverleners tot gevoelige en kritieke data te bewaken
- Er is onvoldoende zekerheid over de kwaliteit van de uitbestede diensten
- Er is onvoldoende inzicht in de eigen concentratierisico's van (onder)uitbesteding.

In Bijlage I van deze brief vindt u een toelichting op deze bevindingen.

DeNederlandscheBank
EUROSYSTEEM

Datum
14 augustus 2018

Ons kenmerk
T039-919612099-216

Verzoek DNB
DNB verzoekt u aan de hand van de bevindingen in deze brief uw eigen uitbestedingsprocessen kritisch tegen het licht te houden.

Tot slot
DNB zal de komende periode meer aandacht besteden aan dit onderwerp. Temeer omdat het de verwachting is dat de inherente risico's op dit vlak in de komende jaren toenemen.

Mocht u vragen hebben over het onderzoek of wilt u uw specifieke situatie bespreken, neemt u dan contact op met uw toezichthouder.

Met vriendelijke groet,
De Nederlandsche Bank N.V.

Mw. Drs. G. van Vollenhoven-Eikelenboom AAG
Divisiedirecteur

Ing. J. Jacobs RE CRISC
Afdelingshoofd

DeNederlandscheBank
EUROSYSTEEM

Bijlage 1: Resultaten van het onderzoek 'Uitbesteding'

Datum
14 augustus 2018

Ons kenmerk
T039-919612099-216

In 2017 heeft DNB door middel van een self-assessment een inventariserend onderzoek uitgevoerd naar uitbesteding en de beheersing van het uitbestedingsrisico bij verzekeraars en pensioenfondsen.

Aanleiding
De aanleiding voor het onderzoek was het vermoeden van een toename in de (cloud) uitbesteding van belangrijke bedrijfsactiviteiten. De druk op kostenreducties en de invloed van FinTech versterkt deze trend mogelijk verder. Maar met de toename van de uitbestede activiteiten kunnen ook de uitbestedingsrisico's toenemen. Cloud-uitbesteding brengt daarbij een aantal additionele risico's met zich mee vanwege de opslaglocatie van de gegevens en de verwerking en beveiliging hiervan.

Opzet van het onderzoek
Het onderzoek is uitgevoerd onder 59 verzekeraars en 37 pensioenfondsen en richtte zich op de uitbesteding van materiële[1] activiteiten[2] naar externe dienstverleners[3]. Daarbij kwam de volledige keten van onderuitbesteding[4] van deze dienstverleners tot en met de laatste schakel van de keten in beeld: de opslag en het beheer van data.

Uitkomsten
Hieronder volgt een toelichting op de belangrijkste bevindingen uit dit onderzoek met betrekking tot pensioenfondsen. De resultaten zijn onderverdeeld in drie categorieën. Deze categorieën komen overeen met die in de self-assessment:

(1) Inherent risico: de mate waarin uitbesteding plaatsvindt en het soort uitbesteding
(2) De beheersing van het uitbestedingsrisico
(3) Concentratierisico bij dienstverleners

(1) Inherent risico: de mate waarin uitbesteding plaatsvindt en het soort uitbesteding.

Bijna alle pensioenfondsen hebben één of meer activiteiten uitbesteed. Pensioenfondsen werken veelal op basis van een model waarbij alle business processen (BPO) zijn uitbesteed aan een pensioenuitvoeringsorganisatie (PUO). PUO's besteden vervolgens ook activiteiten en diensten uit. Het gaat hierbij vooral om financiële- en deelnemersadministraties, datacenter- en infrastructurele services, netwerkbeheer en monitoring en databeheer en datavernietiging.

Het percentage uitbesteding onder pensioenfondsen was de afgelopen jaren hoog (BPO) en stabiel. In de self-assessment geven pensioenfondsen aan dat het percentage uitbesteding de komende jaren stabiel zal blijven, maar dat (onder)uitbesteding toeneemt doordat PUO's meer uitbesteden.

[1] Voor materieel kunt u ook kritiek of belangrijk lezen.
[2] Voor activiteit kunt u ook functie lezen. Het uitgevoerde onderzoek heeft zich echter niet op uitbesteding van (kritieke) functies gericht, alleen op de uitbesteding van activiteiten.
[3] Vermogensbeheer valt buiten scope van dit onderzoek
[4] Activiteiten worden uitbesteed aan andere dienstverleners onder verantwoordelijkheid van een 'hoofddienstverlener'

Het aandeel materiële uitbesteding naar de cloud stijgt eveneens, waardoor een verschuiving in het soort uitbesteding zichtbaar is. Sinds 2011 melden instellingen hun cloud uitbestedingen aan de cloud aan DNB. In 2017 is dit aantal meldingen verdubbeld ten opzichte van 2016; het betreft nu een kwart van alle gerapporteerde contracten aan DNB. Door meer naar de cloud uit te besteden neemt geregeld het aantal onderaannemers toe en daardoor ook het inherente risico. Achtergrond hierbij is dat langere uitbestedingsketens samengaan met een complexe beheersing (onder andere beveiliging en continuïteit van informatie) wat zorgt voor een hoger inherent risico.

(2) De beheersing van het uitbestedingsrisico

Op basis van het self-assessment beheerst een groot deel van de deelnemers aan dit onderzoek de uitbestedingsrisico's onvoldoende. De voornaamste tekortkomingen die uit het onderzoek volgen, zijn:

<u>Uitbestedingen worden niet structureel centraal geregistreerd</u>
Deelnemende pensioenfondsen en PUO's hebben veel inspanning moeten leveren om de benodigde data op te halen bij hun verschillende bedrijfsonderdelen en dienstverleners. In sommige gevallen werd de data uiteindelijk niet verkregen. DNB verwacht dat pensioenfondsen in staat zijn om binnen een redelijke termijn inzicht kunnen krijgen in de uitbestedingen en een centrale registratie van hun uitbestedingspartijen bijhouden.

<u>Het interne beleid voldoet niet bij alle pensioenfondsen aan de wettelijke vereisten</u>
Bij een deel van de pensioenfondsen is het uitbestedingsbeleid nog onvoldoende aangepast op risico's samenhangend met uitbesteding naar de cloud.
Tevens ontbreken in verschillende uitbestedingscontracten de wettelijk verplichte contractclausules, zoals exit-bepalingen, bepalingen voor het 'right to examine' voor DNB en het auditrecht voor interne auditdiensten. Soms ontbreken bepalingen in het contract over de wijze van informatie-uitwisseling, monitoring en controle en evaluatie van de geleverde prestaties.

<u>Bestuurders ontvangen niet op reguliere basis managementinformatie over uitbestedingen inclusief onderaannemers</u>
De frequentie waarop het bestuur managementinformatie ontvangt en deze beoordeelt en vergelijkt met haar eigen 'risk appetite' is laag. Een groot deel van de pensioenfondsen geeft aan niet op reguliere basis informatie te ontvangen. Onderaannemers informeren veelal uitsluitend in het geval van een incident. DNB verwacht dat het bestuur op frequente basis managementinformatie ontvangt over uitbestedingen, inclusief afdoende informatie van eventuele onderuitbestedingen.

<u>Evaluatie van uitbestedingen en dienstverleners schiet tekort</u>
Uitbestedingen en dienstverleners worden niet met een vastgestelde frequentie geëvalueerd, en soms alleen aan het einde van de looptijd van een contract. Daarbij richt de evaluatie zich in enkele gevallen onvoldoende op een aantal van belang zijnde aspecten, zoals financiële situatie van de dienstverlener, de kwaliteit van de onderaannemers en de omvang van de opdracht in relatie tot de omvang van de dienstverlener.

Activiteiten uitgevoerd door serviceproviders worden niet structureel meegenomen bij Business Continuity Management (BCM)
De uitbestede activiteiten zijn veelal niet opgenomen in het eigen bedrijfscontinuïteitsplan. Het merendeel van de fondsen geeft te kennen dat dienstverleners continuïteitsmaatregelen hebben getroffen. DNB verwacht dat activiteiten van dienstverleners standaard onderdeel zijn van het BCM van het fonds.

Er zijn onvoldoende beheersmaatregelen om de toegang van dienstverleners tot gevoelige en kritieke data te bewaken
Het merendeel van de pensioenfondsen geeft aan dat beheersmaatregelen zijn getroffen, maar een significant percentage blijkt geen toegang te hebben tot audittrails of beveiligingslogboeken (securitylogs) bij de dienstverleners.
DNB verwacht dat pensioenfondsen in control zijn over de eigen data, ook ingeval van uitbesteding. Dit gaat dus verder dan de beheersmaatregel zelf, ook gedetailleerd inzicht in de effectiviteit van beheersmaatregelen bij dienstverleners is essentieel.

Er is onvoldoende zekerheid beschikbaar over de kwaliteit van geleverde prestaties door dienstverleners
De service-level-rapportages stellen de pensioenfondsen niet altijd in staat om de kwaliteit van de dienst afdoende vast te stellen. In tegenstelling tot de grote contracten worden voor kleinere (maar nog steeds materiële) contracten niet op een frequente basis service level rapportages ontvangen.

Uit het onderzoek blijkt dat bij pensioenfondsen en PUO's voor een kwart van de uitbestedingscontracten geen assurance beschikbaar is over de kwaliteit van de geleverde prestaties. Een groot deel van de wel beschikbare 'third party' rapportages, wordt als 'goed' beoordeeld maar een aanzienlijk deel van de rapportages wordt niet aantoonbaar geanalyseerd. Bevindingen in dergelijke rapportages worden niet altijd opgevolgd en ook wordt niet altijd beoordeeld of de scope en diepgang van rapportages voldoende dekkend zijn voor de afgenomen diensten. Betrokkenheid van het pensioenfonds middels een eigen audit bij zo'n partij vindt in onvoldoende mate plaats.
DNB verwacht dat pensioenfondsen (en hun PUO's) voldoende inspanningen leveren om de kwaliteit van uitbestedingen te waarborgen, aantoonbaar assurancerapportages analyseren en ook ingrijpen indien de kwaliteit tekort mocht schieten. Pensioenfondsen dienen adequate maatregelen te treffen om de kwaliteit van uitbestedingen te evalueren indien geen afdoende assurancerapportages worden ontvangen.

(3) Concentratierisico bij dienstverleners

Een deel van de pensioenfondsen heeft onvoldoende inzicht in de eigen concentratierisico's van (onder)uitbesteding

De ketens van uitbestedingen door 'onderuitbestedingen' worden langer. Daardoor neemt ook het risico op concentraties bij dienstverleners toe. Onderdeel van het onderzoek was om de ketens van uitbesteding inzichtelijk te maken inclusief de potentiele concentraties bij dienstverleners binnen zo'n keten.
Mede door het ontbreken van een centrale registratie bij de pensioenfondsen, is een deel van de pensioenfondsen en PUO's niet in staat gebleken om alle (onder)uitbestedingen te rapporteren, waardoor de gehele keten niet goed in beeld

is gekomen. Hierdoor is de omvang van het concentratierisico binnen de sector, maar ook per pensioenfonds niet volledig inzichtelijk geworden.

De grote dienstverleners zijn wel in beeld gekomen. De top tien wordt aangevoerd door een aantal traditionele spelers (onder andere infrastructuur- en datacenter services) met daarop volgend een aantal mondiale en nationale cloudproviders.

De toename van cloud uitbesteding zal een wijziging met zich meebrengen in de concentraties op dienstverleners en de risico's die hieraan zijn verbonden. Het inzicht in mogelijke concentratierisico's bij dienstverleners kan worden verbeterd. Hier ligt een uitdaging voor zowel de sector als de toezichthouders. Het beter in beeld brengen van de (onder)uitbestedingen door zowel fondsen als PUO's is hierin een noodzakelijke stap.
DNB verwacht dat fondsen en PUO's alle (onder)uitbestedingen en concentraties centraal registreren en op niveau van het pensioenfonds concentraties bij dienstverleners monitoren en analyseren bij het herzien van de uitbestedingsstrategie.

Tot slot
De resultaten van dit onderzoek laten zien dat ruimte voor verbetering is in de beheersing van de risico's die gepaard gaan met (onder)uitbestedingen.

DNB zal de komende periode meer aandacht besteden aan dit onderwerp. Temeer omdat het de verwachting is dat de inherente risico's op dit vlak in de komende jaren toenemen. DNB gaat ervan uit dat alle pensioenfondsen hun eigen uitbestedingsprocessen kritisch tegen het licht houden, met als hulpmiddel de onderzoeksbevindingen.