DeNederlandscheBank
EUROSYSTEEM

[Naam verzekeraar]
[Adres]

De Nederlandsche Bank N.V.
Toezicht Verzekeraars

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

Handelsregister 3300 3396

Onderwerp
Sectorbrede terugkoppeling verzekeraars 'Inventarisatie Uitbesteding'

Datum
18 juni 2018

Uw kenmerk

Ons kenmerk
T039-919612099-195

Behandeld door
Ingrid Talsma

Bijlagen
1

Geachte [..],

In 2017 heeft DNB een inventariserend 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 uitbestedingen van bedrijfsactiviteiten, waaronder cloud uitbestedingen. Aandacht hiervoor is belangrijk, temeer omdat de verwachting is dat de inherente 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
De resultaten van dit onderzoek laten zien dat er ruimte voor verbetering is voor wat betreft de beheersing van de (onder)uitbestedingsrisico's. De belangrijkste bevindingen zijn hieronder opgenomen:

- Uitbestedingen worden niet structureel centraal geregistreerd.
- Het interne beleid voldoet niet aan de wettelijke vereisten[1].
- Directies ontvangen niet op reguliere basis managementinformatie over uitbestedingen inclusief onderaannemers.
- Evaluatie van serviceproviders behoeft verbetering in zowel frequentie als kwaliteit.
- Activiteiten uitgevoerd door serviceproviders worden niet structureel meegenomen in Business Continuity Management.
- Er zijn onvoldoende beheersmaatregelen om de toegang van serviceproviders tot gevoelige data te bewaken.
- Er is onvoldoende zekerheid beschikbaar over de kwaliteit van geleverde diensten door serviceproviders.
- 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.

Uit eerder DNB onderzoek[2] blijkt dat (significante) beveiligingsrisico's ontstaan wanneer een schakel in de keten de beveiliging niet op het vereiste niveau heeft gebracht: *'De keten is zo sterk als de zwakste schakel'.*
Structurele aandacht van de directie van instellingen is nodig om de risico's van uitbesteding binnen de organisatie effectief te borgen.

[1]Solvency II richtlijn 2009/138/EG, Solvency II Verorderingen 2015/35/EU, EIOPA Richtsnoeren voor het governancesysteem, 60 t/m 64, afd. 11 uitbesteding, Wet op het financieel toezicht, artikel 3.18
[2]Zie sector terugkoppeling resultaten informatiebeveiliging – Cyber onderzoek 2017 - bij verzekeraars en pensioenfondsen (nieuwsbrief verzekeraars februari 2018, www.dnb.nl)

DeNederlandscheBank
EUROSYSTEEM

Datum
15 juni 2018

Ons kenmerk
T039-919612099-195

Verwachtingen DNB
DNB verwacht dat verzekeraars zich bewust zijn en blijven van het feit dat ook bij uitbesteding de verzekeraar eindverantwoordelijk is voor de beheersing van de onderhavige risico's. Alhoewel DNB constateert dat naar aanleiding van dit onderzoek instellingen reeds verbeteringen doorvoeren zal DNB de komende periode meer aandacht besteden aan dit onderwerp. DNB gaat ervan uit dat alle verzekeraars hun eigen uitbestedingsprocessen kritisch tegen het licht houden, met als hulpmiddel de onderzoeksbevindingen en de later dit jaar te verschijnen definitieve Good Practices.

Tot slot
DNB heeft ook concept-Good Practices opgesteld die verzekeraars kunnen gebruiken om de uitkomsten van het onderzoek op te pakken. DNB stelt deze concept-Good Practices open ter consultatie tot en met 30 juni 2018. Deze Good Practices kunt u inzien via http://www.toezicht.dnb.nl/2/50-237170.jsp.
Tot die datum kunt u opmerkingen en onduidelijkheden melden via het e-mailadres inventarisatie_uitbesteding@dnb.nl. Na verwerking van de consultatiereacties zal DNB de definitieve Good Practices op DNB Open Boek Toezicht plaatsen.

Mocht u vragen hebben over het onderzoek of wilt u uw specifieke situatie bespreken, neemt u dan contact op met uw toezichthouder. Alle deelnemende verzekeraars ontvangen een individuele terugkoppeling van het onderzoek via hun toezichthouder.

Met vriendelijke groet,
De Nederlandsche Bank N.V.

Drs. M.W. van Woerden
Divisiedirecteur

Ing. J. Jacobs RE CRISC
Afdelingshoofd

DeNederlandscheBank
EUROSYSTEEM

Bijlage 1: Resultaten van het onderzoek 'Uitbesteding'

Datum
15 juni 2018

Ons kenmerk
T039-919612099-195

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 uitbesteding van bedrijfsactiviteiten: ICT, vermogensbeheer, pensioen- polis- en financiële administraties en andere belangrijke bedrijfsprocessen. 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[3] activiteiten[4] naar externe serviceproviders en de volledige keten van onderuitbesteding[5] van deze serviceproviders tot en met de laatste schakel van de keten: de opslag en het beheer van data.

Uitkomsten
Hieronder volgt een toelichting op de belangrijkste bevindingen uit dit onderzoek met betrekking tot verzekeraars. De resultaten zijn onderverdeeld in drie categorieën conform de self-assessment:

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

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

Het uitbesteden van kritische bedrijfsprocessen (zoals de polis- en financiële administratie) neemt toe, voornamelijk door het gebruik van SaaS (Software as a Service) toepassingen. Uitgedrukt in aantallen contracten worden datacenter services het meest uitbesteed gevolgd door claims- en klachtenafhandeling (schadeafhandeling), applicatiebeheer en infrastructurele services.

Het aandeel materiële uitbesteding naar de cloud stijgt eveneens, waardoor een verschuiving in het soort uitbesteding zichtbaar is. In 2017 is het aantal meldingen van cloud uitbesteding verdubbeld ten opzichte van 2016; het betreft nu een kwart van alle gerapporteerde uitbestedingen 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

[3] Voor materieel kunt u ook kritiek of belangrijk lezen; Richtsnoer 60 v/e Richtsnoeren voor het Governancesysteem.
[4] Voor activ teit kunt u ook functie lezen (artikel 49 Solvency II Richtlijn). Het uitgevoerde onderzoek heeft zich echter niet op uitbesteding van (sleutel)functies gericht, alleen op de uitbesteding van activiteiten.
[5] Activiteiten worden uitbesteed aan andere dienstverlener(s) onder verantwoordelijkheid van een 'hoofddienstverlener'

langere uitbestedingsketens samengaan met een complexe beheersing (onder andere beveiliging van informatie).

Bovenstaande ontwikkelingen zijn in lijn met de verwachting van DNB dat uitbesteding belangrijker wordt en daarmee potentieel ook de risico's toenemen. Het percentage uitbesteding[6] onder verzekeraars in kosten uitgedrukt bleek echter de afgelopen jaren stabiel, in tegenstelling tot de verwachting van DNB. Deelnemende verzekeraars geven verder aan dat het percentage uitbesteding de komende jaren stabiel zal blijven, maar dat het aandeel ICT uitbesteding en onderuitbesteding zal gaan toenemen door veranderingen in uitbestedingsstrategie- en kosten.

(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 zijn gebleken, zijn:

Uitbestedingen worden niet structureel centraal geregistreerd Deelnemende verzekeraars hebben veel inspanning moeten leveren om de benodigde data op te halen bij hun verschillende bedrijfsonderdelen en serviceproviders. In sommige gevallen werd de data uiteindelijk niet verkregen. DNB verwacht dat verzekeraars in staat zijn om binnen een redelijke termijn inzicht te geven in de uitbestedingen en een centrale registratie van hun uitbestedingspartners bijhouden.

Het interne beleid voldoet niet aan de wettelijke vereisten[7]
Bij een deel van de verzekeraars is het uitbestedingsbeleid nog onvoldoende aangepast op risico's samenhangend met uitbesteding naar de cloud. Tevens ontbreken in verschillende uitbestedingscontracten de wettelijk verplichte contractclausules (onder andere separate exitbepalingen, bepalingen voor het 'right to examine' voor DNB en het 'right to audit' voor een interne- en externe auditdienst).
DNB verwacht dat ontbrekende clausules worden toegevoegd en tevens dat het beleid periodiek wordt geëvalueerd en zo nodig wordt herzien.

Directies ontvangen niet op reguliere basis managementinformatie over uitbestedingen, zowel voor wat betreft de hoofddienstverlener als van haar onderaannemers
De frequentie waarop de directie managementinformatie ontvangt en deze beoordeelt en vergelijkt met haar eigen 'risk appetite' is laag. De helft van de verzekeraars geeft aan niet op reguliere basis stuurinformatie te ontvangen. Onderaannemers informeren veelal uitsluitend in het geval van een incident. DNB verwacht dat directies op frequente basis managementinformatie ontvangen over uitbestedingen, inclusief afdoende informatie van eventuele onderaannemers.

Evaluatie van serviceproviders behoeft verbetering in zowel frequentie als kwaliteit
Diensten van een serviceprovider worden niet met een vastgestelde frequentie geëvalueerd, maar soms pas aan het einde van de looptijd van een contract. Daarbij richt de evaluatie zich in enkele gevallen onvoldoende op een aantal van

[6] Uitbestedingsratio wordt berekend als aandeel van de kosten voor uitbesteding op de totale algemene operationele kosten van de verzekeraar.
[7] Solvency II richtlijn 2009/138/EG, Solvency II Verorderingen 2015/35/EU, EIOPA Richtsnoeren voor het governancesysteem, 60 t/m 64 in afdeling 11 over uitbesteding

belang zijnde aspecten. DNB verwacht dat de diensten van een serviceprovider met een vastgestelde frequentie worden geëvalueerd gericht op voldoende relevante aspecten.

Activiteiten uitgevoerd door serviceproviders worden niet structureel meegenomen bij Business Continuity Management (BCM)
Bij ruim de helft van de contracten worden activiteiten uitgevoerd door serviceproviders niet meegenomen in uitwijkplannen (BCP). Bij 30% van de verzekeraars is de serviceprovider wel actief betrokken bij het testen van BCM-plannen. Slechts een kwart maakt een scenario-analyse als onderdeel van BCM waarin de uitbestede diensten zijn betrokken.
DNB verwacht dat activiteiten van serviceproviders standaard onderdeel zijn van BCM.

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

Er is onvoldoende zekerheid beschikbaar over de kwaliteit van geleverde diensten door serviceproviders
De service level rapportages stellen de instelling 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 voor bijna 40% van de contracten geen assurancerapportages beschikbaar zijn. Een groot deel van de rapportages die wel beschikbaar zijn, wordt door de verzekeraar als 'goed' beoordeeld maar een aanzienlijk deel van de rapportages wordt niet aantoonbaar geëvalueerd. 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 dienstverlening. Betrokkenheid middels een eigen audit bij de serviceprovider vindt in onvoldoende mate plaats.
DNB verwacht dat verzekeraars voldoende inspanningen leveren om de kwaliteit van uitbestedingen te waarborgen, aantoonbaar assurancerapportages evalueren en ook ingrijpen indien de kwaliteit tekort mocht schieten. Verzekeraars dienen adequate maatregelen te treffen om de kwaliteit van uitbestedingen te evalueren indien geen afdoende assurancerapportages worden ontvangen.

(3) Concentratierisico bij serviceproviders

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

Mede door het ontbreken van een centrale registratie, is een deel van de instellingen 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 verzekeringssector, maar ook per instelling niet volledig inzichtelijk geworden.

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

De toename van cloud uitbesteding zal een wijziging met zich mee brengen in de concentraties op serviceproviders en de risico's die hieraan verbonden zijn. DNB verwacht dat verzekeraars concentraties centraal registreren en op instellingsniveau 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.

Alhoewel DNB constateert dat naar aanleiding van dit onderzoek instellingen reeds verbeteringen doorvoeren zal DNB 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 verzekeraars hun eigen uitbestedingsprocessen kritisch tegen het licht houden.

DNB heeft ook concept-Good Practices opgesteld die verzekeraars kunnen gebruiken om de uitkomsten van het onderzoek op te pakken. DNB stelt deze concept-Good Practices open ter consultatie tot en met 30 juni 2018. Deze Good Practices kunt u inzien via http://www.toezicht.dnb.nl/2/50-237170.jsp.
Tot die datum kunt u opmerkingen en onduidelijkheden melden via het e-mailadres inventarisatie_uitbesteding@dnb.nl. Na verwerking van de consultatiereacties zal DNB de definitieve Good Practices op DNB Open Boek Toezicht plaatsen.