# Good Practice

## Uitbesteding Verzekeraars

DeNederlandscheBank
EUROSYSTEEM

# Inhoud

# Inleiding



Verzekeraars besteden ICT, vermogensbeheer, pensioen- polis- en financiële administraties en andere belangrijke bedrijfsprocessen uit, bijvoorbeeld om te profiteren van de kennis en schaalgrootte van een dienstverlener en zo de kosten te reduceren óf om te focussen op de kerncompetenties. Tegenover deze voordelen staan ook risico's waar een verzekeraar zich aan blootstelt bij het uitbesteden van activiteiten en functies. Bijvoorbeeld het risico dat de continuïteit en betrouwbaarheid van de bedrijfsvoering in gevaar komt door contractbreuk, financiële problemen van de dienstverlener of ongewenste omgang met vertrouwelijke gegevens of het risico dat kwaliteit van de geleverde service niet in overeenstemming is met de toegezegde kwaliteit. Deze Good Practice bevat handvatten voor verzekeraars om deze en andere uitbestedingsrisico's te beheersen.

## Relevante wet- en regelgeving

Deze Good Practice bevat handvatten voor de volgende wet- en regelgeving die relevant is wanneer een verzekeraar werkzaamheden uitbesteedt:

- Wet op het financieel toezicht (Wft)
  - Artikel 1:1; definities
  - Artikel 3:17; beheerste en integere bedrijfsvoering
  - Artikel 3:18; uitbesteding
- Besluit prudentiele regels (Bpr)
  - Artikelen 27 tot en met 32 over het uitbesteden van werkzaamheden
- Solvency II Richtlijn 2009/138/EG
  - Artikel 13(28): definitie van uitbesteding
  - Artikel 38: toezicht op uitbestede functies en werkzaamheden
  - Artikel 41: algemene governance vereisten
  - Artikel 49: uitbesteding
- Solvency II Verordeningen 2015/35/EU
  - Artikel 258: algemene governance vereisten
  - Artikel 274: uitbesteding
- EIOPA Richtsnoeren voor het governancesysteem
  - Richtsnoeren 60 tot en met 64 in afdeling 11 over uitbesteding (niet van toepassing op Basic verzekeraars)

## Definities

Artikel 1.1. van de Wet op het financieel toezicht definieert uitbesteden als het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden:

- die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten; of
- die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan;

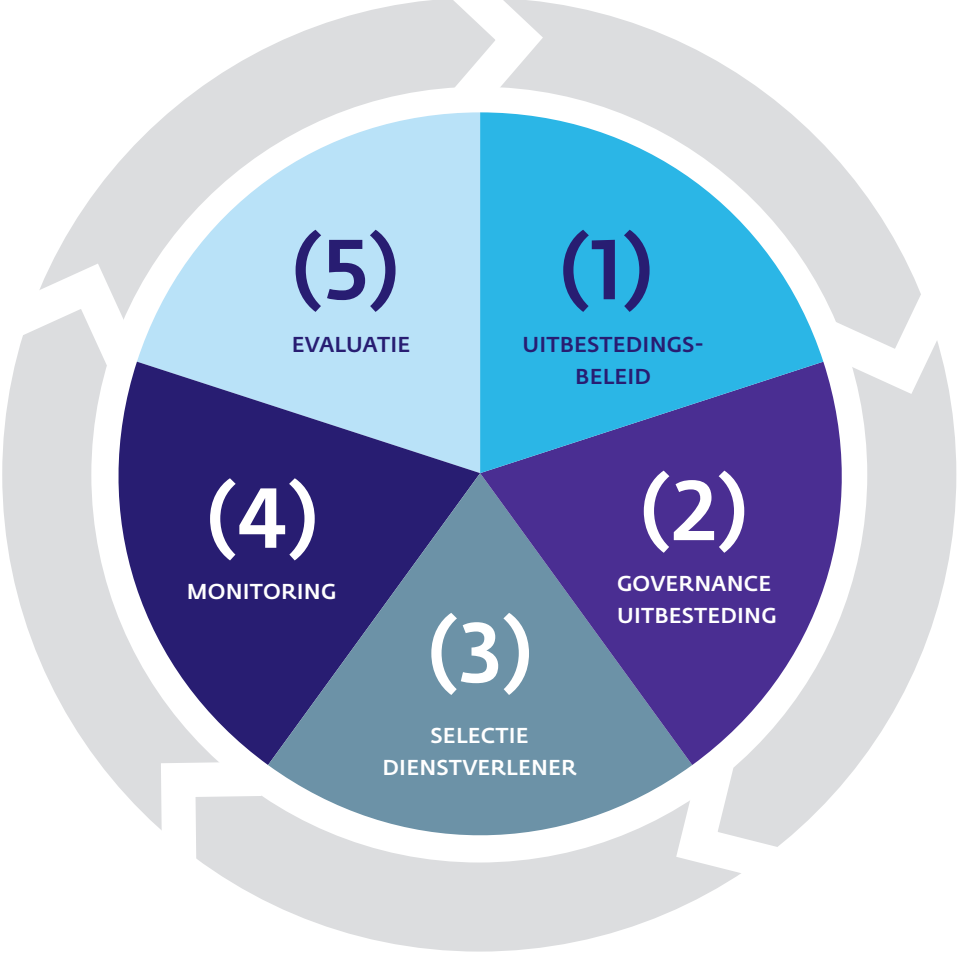
Artikel 13.28 van de Solvency II Richtlijn 2009/138/EG definieert uitbesteding als een overeenkomst van om het even welke vorm tussen een verzekeraar en een al dan niet onder toezicht staande dienstverlener op grond waarvan deze dienstverlener hetzij rechtstreeks hetzij door middel van onderuitbesteding een proces, een dienst of een activiteit uitvoert die anders door de verzekeraar zelf zou worden uitgevoerd.

## Fases uitbestedingsproces

De good practices voor uitbesteding beslaan vijf fases in het uitbestedingsproces:

1. Uitbestedingsbeleid: de overwegingen op grond waarvan tot uitbesteding kan worden besloten en de randvoorwaarden waaronder dit plaatsvindt. Hoe geeft de verzekeraar invulling aan de uitbesteding én hoe beheerst de verzekeraar de uitbestedingsrisico's.
2. Inrichten Governance en Opstellen Uitbestedingsovereenkomst: het beleid is richtinggevend en kaderstellend. Het vertaalt zich uiteindelijk naar een uitbestedingsovereenkomst die voldoet aan alle wettelijke vereisten en de eisen en wensen van de verzekeraar.
3. Selectie dienstverlener: hoe selecteert de verzekeraar een dienstverlener.
4. Monitoring uitbesteding: hoe houdt de verzekeraar in de gaten dat de dienstverlener doet wat in de overeenkomst staat en zich aan de performance en resultaatafspraken houdt.
5. Evaluatie uitbesteding: periodiek evalueert de verzekeraar het functioneren van de dienstverleners en haar beleid en processen in alle stappen van het uitbestedingsproces; afhankelijk van de uitkomsten neemt de verzekeraar corrigerende maatregelen, selecteert een andere dienstverlener of past het beleid voor uitbesteding aan.

## Figuur 1 Vijf fases van het uitbestedingsproces




Een beheerste bedrijfsvoering omvat het hele traject van plannen, sturen, monitoren en bijsturen van doelstellingen, processen en risico's. Deze cyclus (Plan, Do, Check, Act) is ook toepasbaar op het uitbestedingsproces en laat zich vertalen in de vijf fases van het uitbestedingsproces.

In de volgende hoofdstukken leest u welke good practices DNB ziet bij de bovenstaande fases in het uitbestedingsproces. Een hoofdstuk begint met een korte tekst als inleiding op de voor dit onderwerp relevante wet- en regelgeving gevolgd door good practices. Niet voor alle wet- en regelgeving vindt u good practices hoe een verzekeraar invulling kan geven aan deze wettelijke vereisten. Dat neemt niet weg dat verzekeraars wel aan alle wettelijke eisen behoren te voldoen. De wet- en regelgeving is weergegeven in kaders.

## Scope

De Good Practice heeft betrekking op belangrijke, kritieke uitbestedingen. Met belangrijke, kritieke uitbesteding wordt bedoeld een uitbesteding die materieel of van wezenlijk belang is. De impact van het uitbesteden is hiervoor bepalend. Aangezien dit van de omstandigheden afhangt, zijn er verschillen per verzekeraar.
Niet alle voorbeelden zijn toepasbaar bij alle verzekeraars. Verzekeraars maken eigen afwegingen welke maatregel past bij het specifieke risico. Basic verzekeraars kunnen mogelijk volstaan met andere maatregelen dan grote verzekeraars. De Richtsnoeren voor het governancesysteem zijn bijvoorbeeld niet van toepassing op Basic verzekeraars. Binnen concerns kunnen verschillen optreden door diversiteit van de bedrijfsonderdelen, zowel wat betreft activiteiten als strategie. Een verzekeraar kan een proportionaliteitstoets onderdeel laten uitmaken van de risicoanalyse.

Deze Good Practice kan worden gebruikt bij de uitbesteding van kritieke of belangrijke functies, maar biedt geen handvatten specifiek gericht op de beheersing hiervan. Kritieke of belangrijke functies zijn fundamenteel voor het vermogen van de verzekeraar om haar kernactiviteit uit te oefenen. De impact van het uitbesteden is bepalend voor de vraag of een functie kritiek of belangrijk is. In ieder geval vallen de in artikel 41, 44, 46 en 47 van de Solvency II Richtlijn genoemde functies onder de kritieke functies (sleutelfuncties): risicomanagementfunctie, compliancefunctie, interne auditfunctie en actuariële functie.

### Richtsnoer 60 – Kritieke of belangrijke operationele functies of activiteiten

1.113 De onderneming moet vaststellen of, en documenteren dat, een uitbestede functie of activiteit een kritieke of belangrijke functie of activiteit is. Dit dient te geschieden aan de hand van de vraag of de betreffende functie of activiteit van essentieel belang is voor de bedrijfsvoering van de onderneming in de zin dat de onderneming zonder deze functie of activiteit niet in staat zou zijn om haar diensten aan de verzekeringnemers te verlenen.

Bij de beheersing van uitbesteding van ICT en data kan een verzekeraar gebruik maken van het toetsingskader Informatie Beveiliging waarin een specifieke set aan controlemaatregelen gericht op uitbesteding is opgenomen. Bijvoorbeeld Managed

third party and supplier services (14.1 en 14.2) en Monitoring (bv 16.3)

De Good Practice richt zich op de nadere invulling van de prudentiële regelgeving, Artikel 4.16 Wft (gedragstoezicht) is hier geen onderdeel van. Verzekeraars kunnen in hun hoedanigheid als adviseur/bemiddelaar hun voordeel doen met deze Good Practice.

Onder uitbesteding wordt mede verstaan het verlenen van een volmacht aan een tussenpersoon (gevolmachtigd agent). De verzekeraar moet er voor zorgen dat de activiteiten van deze tussenpersoon voldoen aan de uitbestedingsvereisten.

### Richtsnoer 61 – Aangaan van verzekeringstechnische verplichtingen

1.114 De onderneming moet ervoor zorgen dat de activiteiten van een tussenpersoon (volmachthouder) die geen werknemer van de onderneming is en die gemachtigd is om namens en voor rekening van onderneming verzekeringen af te sluiten en schaden uit te keren, voldoen aan de uitbestedingsvereisten.

Uitbesteding binnen een groep valt ook binnen de scope van deze Good Practice.

### Richtsnoer 62 – Uitbesteding binnen een groep

1.115 Indien kritieke of belangrijke functies of activiteiten binnen de groep worden uitbesteed, moeten de deelnemende verzekerings- of herverzekeringsonderneming, de verzekeringsholding of de gemengde financiële holding documenteren welke functies verband houden met welke rechtspersoon. Daarnaast moet die entiteit waarborgen dat door dergelijke regelingen geen afbreuk wordt gedaan aan de uitvoering van die kritieke of belangrijke functies of activiteiten op het niveau van de onderneming.

# 1. Uitbestedingsbeleid

Zonder beleid geen uitbesteding. Voor een verzekeraar overgaat tot uitbesteding legt een verzekeraar een uitbestedingsbeleid vast. Dit beleidsdocument bevat de overwegingen op grond waarvan tot uitbesteding kan worden besloten en de randvoorwaarden waaronder de uitbesteding plaatsvindt. Uitgangspunt: de verzekeraar is en blijft volledig verantwoordelijk.

## Artikel 49 – Uitbesteding Richtlijn 2009/138/EG

1. De lidstaten zorgen ervoor dat verzekerings- en herverzekeringsondernemingen bij de uitbesteding van functies of van verzekerings- of herverzekeringswerkzaamheden volledig verantwoordelijk zijn voor de nakoming van al hun verplichtingen uit hoofde van deze richtlijn
2. Uitbesteding van kritieke of belangrijke operationele functies of werkzaamheden mag niet tot het volgende leiden:
   a. Er wordt wezenlijk afbreuk gedaan aan de kwaliteit van het governancesysteem van de betrokken onderneming
   b. Het operationele risico neemt onnodig toe
   c. Er wordt afbreuk gedaan aan het vermogen van de toezichthoudende autoriteiten om te controleren of de onderneming haar verplichtingen nakomt
   d. De continuïteit en toereikendheid van de dienstverlening aan de verzekeringnemers wordt ondermijnd.
3. Vóór de uitbesteding van kritieke of belang rijke functies of werkzaamheden stellen verzekerings- en herverzekeringsonder-nemingen de toezichthoudende autoriteiten daarvan en van latere wezenlijke ontwikkelingen met betrekking tot deze functies of werkzaamheden tijdig in kennis.



## 1.1 Beleidsproces

Een verzekeraar legt schriftelijk een uitbestedings-beleid vast, waarin zij rekening houdt met het effect van uitbesteding op haar bedrijfsvoering en past hierbij het proportionaliteitsbeginsel toe. In het uitbestedingsbeleid komen alle fases van het uitbestedingsproces aan bod. Het beleid beschrijft verder hoe de uitbesteding in de bedrijfsstrategie past, welke uitbestedingsrisico's er ontstaan én hoe de verzekeraar deze risico's beheerst. De verzekeraar voert een systematische risicoanalyse uit alvorens te gaan uitbesteden. Een proportionaliteitstoets kan een onderdeel vormen van de risicoanalyse.

### Wettelijk kader

Artikel 274(1) van de Solvency II Verordeningen vraagt de verzekeraar een schriftelijk uitbestedingsbeleid vast te leggen waarin zij rekening houdt met de bij de uitbesteding te treffen rapportage- en controleregelingen. In het beleid beschrijft de verzekeraar de aanpak en processen die van toepassing zijn op de uitbesteding, waarbij met name aandacht wordt besteed aan aspecten genoemd

in Richtsnoer 63 van het governancesysteem: materialiteitsassesment, selectieproces, contractering, monitoring- en evaluatieproces en het business continuity proces van de verzekeraar zelf.

### Richtsnoer 63 – Schriftelijke beleidslijn inzake uitbesteding

1.116 De onderneming die activiteiten of functies uitbesteedt of die voornemens is om dat te gaan doen, moet in haar beleidslijn inzake uitbesteding de aanpak en processen die van toepassing zijn op de uitbesteding bestrijken en wel gedurende de volledige looptijd van de betreffende overeenkomst. In dat beleid moet met name aandacht worden besteed aan de volgende aspecten:

a. Het proces ter bepaling of een functie of activiteit een kritieke of belangrijke functie of activiteit is
b. De wijze waarop een dienstverlener van een adequaat kwaliteitsniveau wordt geselecteerd en hoe en met welke frequentie de prestaties en resultaten van de dienstverlener worden beoordeeld
c. De gegevens die in de schriftelijke overeenkomst met de dienstverlener moeten worden opgenomen, rekening houdend met de eisen die in Gedelegeerde Verordening 2015/35 van de Commissie worden gesteld
d. Noodplannen met het oog op de continuïteit van de bedrijfsvoering, met inbegrip van exit-strategieën voor uitbestede kritieke of belangrijke functies of activiteiten

**Good practices**

Een verzekeraar definieert een doelstelling en scope voor de uitbesteding; wat besteedt een verzekeraar uit en wat niet, én waarom? Een verzekeraar legt deze doelstellingen en overwegingen vast inclusief de randvoorwaarden waaronder dit plaatsvindt. Waar mogelijk legt de verzekeraar vast wat de overwegingen zijn om een uitbesteding te beëindigen.

Een verzekeraar definieert een uitbestedings-strategie waarmee zij haar doelstellingen kan behalen en betrekt bij te maken keuzes, de risico's die hiermee samen gaan én de wijze waarop zij deze risico's doorlopend beheerst.

Het uitbestedingsbeleid omvat alle aspecten van uitbesteding. Bij het opstellen van het uitbestedingsbeleid betrekt een verzekeraar alle relevante afdelingen zoals riskmanagement, juridische zaken, compliance, de betrokken business onderdelen en indien van toepassing de afdelingen IT en Operations.

De uitbestedingsrichtlijnen- en procedures die een verzekeraar gebruikt (businessonderdelen, ICT, volmachthouders) sluiten aan bij het algemene uitbestedingsbeleid van een verzekeraar. De verzekeraar communiceert het beleid naar de medewerkers.

Het uitbestedingsbeleid beschrijft het selectieproces; het bevat de voorwaarden, selectiecriteria en besluitvormingsmomenten die hierbij komen kijken. De verzekeraar neemt in het uitbestedingsbeleid ook een omschrijving op van het evaluatieproces van geselecteerde dienstverleners en legt vast wat er minimaal in de contracten wordt vastgelegd.

Om te beoordelen of een uitbesteding materieel (belangrijk, kritiek) is, voert een verzekeraar zelf een materialiteitsassessment uit. Met belangrijke, kritieke uitbesteding wordt bedoeld een uitbesteding die van wezenlijk belang is. De impact van het uitbesteden is hiervoor bepalend. Aangezien dit van de omstandigheden afhangt, zijn er verschillen per verzekeraar. Een verzekeraar gebruikt de volgende criteria bij de beoordeling van de uitbesteding:

- Het kritisch karakter en het profiel van inherente risico's van de uit te besteden activiteit, dat wil zeggen de vraag of de activiteit essentieel is voor de bedrijfsvoering / bedrijfscontinuiteit / levensvatbaarheid van de verzekeraar en haar verplichtingen jegens haar klanten / polishouders (in de zin dat de onderneming zonder deze functie of activiteit niet in staat zou zijn om haar diensten aan de verzekeringsnemers te verlenen)
- het operationele effect van onderbrekingen en de daarmee gepaard gaande juridische risico's en reputatierisico.
- het effect dat een verstoring van de activiteit kan hebben op de verwachte inkomsten van de verzekeraar.
- het effect dat een schending van vertrouwelijkheid, integriteit of beschikbaarheid van de gegevens kan hebben op de verzekeraar en haar polishouders.

Een verzekeraar die onderdelen van activiteiten uitbesteed met hoge impact op een deel van de polishouders classificeert deze activiteit als kritiek omdat deze verzekeraar zonder deze functie of activiteit niet in staat is om haar diensten aan dit deel van de verzekeringnemers te verlenen. De (prudentiële) impact is bepalend of sprake is van een kritieke uitbesteding

De directie van een verzekeraar accordeert het beleid; de Raad van Commissarissen of ander toezichthoudend orgaan toetst het beleid.

## 1.2 Business Continuity Management (BCM)

Een verzekeraar richt het Business Continuity Management (BCM) in op basis van het opgestelde BCM beleid en -strategie. Hoewel dienstverleners alles in het werk zullen stellen om te allen tijde de uitbestede werkzaamheden uit te kunnen blijven voeren voor de verzekeraar, kan er onverhoopt toch iets misgaan. Om dergelijke situaties het hoofd te bieden stelt een verzekeraar een business continuïteitsplan op waarin ook alle uitbestedingen zijn opgenomen. Dienstverleners zullen ook hun eigen business continuïteitsplannen hebben.

## Wettelijk kader

### Artikel 41.4 – Algemene Governance vereisten Richtlijn 2009/138/EG

Verzekerings- en herverzekeringsondernemingen treffen redelijke maatregelen, waaronder de ontwikkeling van noodplannen, om voor continuïteit en regelmatigheid in de verrichting van hun werkzaamheden te zorgen. Daartoe maakt de onderneming gebruik van passende en proportionele systemen, middelen en procedures.

### Artikel 274.5 – Solvency II verordeningen 3015/35/EU

De verzekerings- of herverzekeringsonderneming die kritieke of belangrijke operationele functies of werkzaamheden uitbesteedt, voldoet aan alle volgende vereisten:

a. Zij zorgt ervoor dat de relevante aspecten van het risicomanagement- en interne controlesysteem van de dienstverlener adequaat genoeg zijn om de naleving van artikel 49, lid 2, onder a) en b), van Richtlijn 2009/138/EG te waarborgen
b. Zij houdt in haar risicomanagement- en interne controlesysteem afdoende rekening met de uitbestede werkzaamheden om de naleving van artikel 49, lid 2, onder a) en b), van Richtlijn 2009/138/EG te waarborgen
c. Zij verifieert of de dienstverlener over de vereiste financiële draagkracht beschikt om de extra taken op behoorlijke en betrouwbare wijze te vervullen, en of alle medewerkers van de dienstverlener die bij de uitvoering van de uitbestede functies of werkzaamheden betrokken zullen zijn, voldoende gekwalificeerd en betrouwbaar zijn
d. Zij zorgt ervoor dat de dienstverlener over adequate noodplannen beschikt om met noodsituaties of bedrijfsonderbrekingen om te gaan, en periodieke tests van back-upvoorzieningen verricht waar zulks noodzakelijk is in het licht van de uitbestede functies en werkzaamheden.

### Richtsnoer 63 – Schriftelijke beleidslijn inzake uitbesteding

1.116 De onderneming die activiteiten of functies uitbesteedt of die voornemens is om dat te gaan doen, moet in haar beleidslijn inzake uitbesteding de aanpak en processen die van toepassing zijn op de uitbesteding bestrijken en wel gedurende de volledige looptijd van de betreffende overeenkomst. In dat beleid moet met name aandacht worden besteed aan de volgende aspecten:

d. Noodplannen met het oog op de continuïteit van de bedrijfsvoering, met inbegrip van exit-strategieën voor uitbestede kritieke of belangrijke functies of activiteiten

**Good practices**

Een verzekeraar definieert en neemt besluiten over continuïteitsmaatregelen. De uitbestede materiële activiteiten vormen onderdeel van deze continuïteitsmaatregelen. Dit houdt in dat zowel de dienstverlener als de verzekeraar continuïteitsmaatregelen neemt aansluitend bij het risicoprofiel van data en systemen, daaronder begrepen back-upvoorzieningen op verschillende locaties op passende afstand van elkaar.

Een verzekeraar stelt een businesscontinuïteitsplan (BCP) op waarin de uitbestede activiteiten zijn opgenomen en de consequenties van een verstoring bij de eigen organisatie of de dienstverleners en welke maatregelen er voorhanden zijn om de gevolgen van deze verstoring tot een minimum te beperken.

Een verzekeraar toetst periodiek in samenwerking met de dienstverleners of de continuïteitsplannen- en maatregelen in een uitbestedingsketen op elkaar aansluiten. De verzekeraar analyseert afwijkingen ten opzichte van de eisen en neemt corrigerende maatregelen. Indien nodig wordt het continuïteitsplan bijgesteld. Op deze manier mitigeert de verzekeraar het risico dat bij een verstoring van één schakel in de keten, de gehele keten niet meer functioneert.

Een verzekeraar test de businesscontinuïteits-maatregelen periodiek, waar mogelijk met de actieve betrokkenheid van de dienstverlener(s) waaraan werkzaamheden zijn uitbesteed.

De verzekeraar volgt daarbij ook de resultaten van door de dienstverlener zelfstandig uitgevoerde BCP-tests.

Een verzekeraar zoekt alternatieve oplossingen voor uitbestede activiteiten en ontwikkelt en implementeert exit- en overgangsplannen aan de hand van de opgestelde exit-strategieën. Een verzekeraar maakt afspraken met de dienstverlener over wat er met de data gebeurt na beëindiging van de uitbesteding. Ook wijst de verzekeraar taken en verantwoordelijkheden toe voor het beheer van deze plannen en de uit te voeren overgangsactiviteiten bij een daadwerkelijke exit, omvattende het retourneren en vernietigen van opgeslagen data (productie en back-up) bij de verlaten dienstverlener.

Een verzekeraar voert scenarioanalyses uit waarin de uitbestede diensten zijn betrokken om na te gaan wat de impact van de bedrijfsschade is bij verschillende scenario's, zoals bijvoorbeeld een natuurramp, brand, DDoS, cybercrime (malware, ransomware etc.)

Bij een besluit om een dienstverlener te verlaten (exit) gaat de verzekeraar na welke middelen nodig zijn om de uitbestede activiteiten over te brengen naar een alternatieve dienstverlener of om deze weer zelf te gaan verrichten (het exit-plan uitvoeren). Een verzekeraar houdt zelf voldoende kennis beschikbaar om de door de dienstverlener geleverde prestatie op waarde te kunnen schatten, goed aan te kunnen sturen, bij te sturen en indien nodig ook weer zelf over te nemen.

Een verzekeraar stelt al dan niet in samenwerking met klanten van dezelfde dienstverlener exit plannen op in het geval dat een dienstverlener niet meer kan leveren door bijvoorbeeld een faillissement. Bij een faillissement is de verzekeraar afhankelijkheid van de door de curator gewenste maatregelen.

Een verzekeraar richt monitoring in ten aanzien van de werking en effectiviteit van de BCM- en BCP-maatregelen van de dienstverlener. Daarnaast is de monitoring van de verzekeraar gericht op het tijdig verzamelen van gegevens die een indicatie kunnen zijn van een verminderde prestatie of continuïteit.

# 2. Governance uitbesteding en uitbestedingsovereenkomst

Het beleid voor uitbesteding en de governance daaromheen is richtinggevend en kaderstellend; het vertaalt zich uiteindelijk naar een uitbestedingsovereenkomst die voldoet aan alle wettelijke vereisten, randvoorwaarden en de eisen en wensen van de verzekeraar. De taken en verantwoordelijkheden van de verzekeraar enerzijds en de dienstverlener anderzijds zijn omschreven en vastgelegd.

## 2.1 Voldoen aan wettelijke vereisten bij uitbesteding

Het uitbestedingsbeleid waarborgt dat voor activiteiten die zijn uitbesteed blijvend wordt voldaan aan alle wettelijke vereisten. Dit 'beleidskader' geeft de voorwaarden en vereisten waaronder mag worden uitbesteed en de grenzen waarbinnen verplichtingen mogen worden aangegaan. De directie waarborgt dat de verzekeraar voldoet aan wet- en regelgeving.

**Wettelijk kader**

### Artikel 274.1 / 274.2 / 274.3 – Solvency II Verordeningen 3015/35/EU

1. Een verzekerings- of herverzekeringsonderneming die functies of verzekerings- of herverzekeringswerkzaamheden uitbesteedt of voornemens is uit te besteden aan een dienstverlener, legt schriftelijk een uitbestedingsbeleid vast waarin rekening wordt gehouden met het effect van uitbesteding op haar bedrijfsvoering en met de bij uitbesteding te treffen rapportage- en controleregelingen. De onderneming draagt er zorg voor dat de voorwaarden van de uitbestedingsovereenkomst in overeenstemming zijn met de verplichtingen van de onderneming uit hoofde van artikel 49 van Richtlijn 2009/138/EG
2. Wanneer de verzekerings- of herverzekeringsonderneming en de dienstverlener tot dezelfde groep behoren, houdt de onderneming bij de uitbesteding van kritieke of belangrijke operationele functies of werkzaamheden rekening met de mate waarin de onderneming zeggenschap heeft over de dienstverlener of invloed kan uitoefenen op diens handelingen.
3. Bij de keuze van de in lid 1 bedoelde dienstverlener voor kritieke of belangrijke operationele functies of werkzaamheden, zorgt het bestuurlijk, beleidsbepalend of toezichthoudend orgaan voor het volgende:
   a. Er wordt diepgaand onderzoek verricht om te waarborgen dat de potentiële dienstverlener over de bekwaamheid, de capaciteit en elke bij wet vereiste vergunning beschikt om de vereiste functies of werkzaamheden op bevredigende wijze uit te voeren, rekening houdend met de doelstellingen en behoeften van de onderneming
   b. De dienstverlener heeft al het nodige gedaan om te voorkomen dat daadwerkelijke of potentiële belangenconflicten de behoeften van de uitbestedende onderneming doorkruisen

c. Tussen de verzekerings- of herverzekeringsonderneming en de dienstverlener wordt een schriftelijke overeenkomst gesloten waarin de respectieve rechten en plichten van de onderneming en de dienstverlener duidelijk omschreven zijn
d. De algemene voorwaarden van de uitbestedingsovereenkomst worden duidelijk uitgelegd aan het bestuurlijk, beleidsbepalend of toezichthoudend orgaan van de onderneming, dat ermee instemt
e. De uitbesteding heeft geen inbreuk op enigerlei wet, en met name de regelgeving inzake gegevensbescherming
f. De dienstverlener is aan dezelfde voorschriften inzake de veiligheid en de vertrouwelijkheid van informatie betreffende de verzekerings- of herverzekeringsonderneming of de verzekeringnemers of begunstigden daarvan onderworpen als die welke voor de verzekerings- of herverzekeringsonderneming gelden.

Artikel 49.3 van de Solvency II Richtlijn en Richtsnoer 64 van de EIOPA Richtsnoeren over het governancesysteem beschrijven dat een verzekeraar DNB tijdig in kennis stelt van een materiële uitbesteding, zodat DNB kan nagaan of het voornemen op prudentiële bezwaren stuit. In de schriftelijke melding staat een beschrijving van de reikwijdte en de redenen voor de uitbesteding en de naam van de dienstverlener.

## Artikel 49 – Uitbesteding Richtlijn 2009/138/EG

3. Vóór de uitbesteding van kritieke of belangrijke functies of werkzaamheden stellen verzekerings- en herverzekeringsondernemingen de toezichthoudende autoriteiten daarvan en van latere wezenlijke ontwikkelingen met betrekking tot deze functies of werkzaamheden tijdig in kennis.

## Richtsnoer 64 – Schriftelijke kennisgeving aan de toezichthoudende autoriteit

1.117 De onderneming moet in haar schriftelijke kennisgeving van een uitbesteding van kritieke of belangrijke functies of activiteiten aan de toezichthoudende autoriteit een beschrijving van de reikwijdte en de redenen voor de uitbesteding en de naam van de dienstverlener opnemen. Wanneer de uitbesteding een sleutelfunctie betreft, moet de informatie ook de naam van de persoon die bij de dienstverlener de leiding heeft over de uitbestede functie of activiteiten bevatten.

### Good practices

Een verzekeraar legt in haar beleid vast dat zij DNB schriftelijk op de hoogte stelt van de uitbesteding van materiële, kritieke activiteiten en van belangrijke wijzigingen in uitbestedingsovereenkomsten, daaronder begrepen onderuitbesteding.

Een verzekeraar meldt de uitbesteding bij DNB minimaal 6 weken voor de in productie name. Ook bij een fasegewijze of project implementatie.

Een verzekeraar omschrijft de taken, bevoegdheden en verantwoordelijkheden en treft waarborgen dat voldoende deskundigheid binnen de verzekeraar aanwezig is om te voorkomen dat de verzekeraar niet langer voldoet aan relevante wet- en regelgeving bij het aangaan van uitbestedingsovereenkomsten, daaronder begrepen onderuitbesteding.

Een verzekeraar formuleert in het beleid dat adequate monitoring nodig is bij uitbesteding. Voor het monitoren van grotere uitbestedingen richt een verzekeraar een regieorganisatie in en beschrijft de benodigde kennis en competenties om de dienstverlener tegenwicht te geven en in het uiterste geval rechtstreeks de leiding over de uitbestede activiteit terug te nemen.

Een verzekeraar is in staat om de dienstverlener bij te sturen en aanvullende of nieuwe afspraken te maken over de door de dienstverlener geleverde prestaties en resultaten (Deming Cycle: Plan > Do > Check > Act). De verzekeraar heeft al bij aanvang van de uitbesteding alternatieven voor de uitbesteding. Dit kan betekenen migreren naar een andere dienstverlener of inbesteding.

Het beleid van een verzekeraar waarborgt dat uitbesteding enkel mogelijk is als het beleid van de dienstverlener minimaal gelijkwaardig (of hoger) is aan het intern beleid van de verzekeraar voor informatiebeveiliging en Business Continuity Management (BCM) of dat er alternatieve maatregelen bestaan om het gewenste resultaat te borgen en er geen onacceptabele risico's bestaan.

Een verzekeraar neemt in het beleid op dat zij de classificatie en beveiliging van systemen en data in haar risicobeoordeling mee neemt. In de schriftelijke overeenkomst met de dienstverlener neemt de verzekeraar clausules inzake beveiliging en gegevensbescherming op, inclusief een verwerkersovereenkomst. Hierbij houdt de verzekeraar rekening met compliance aan de van toepassing zijnde wet- en regelgeving, daaronder begrepen de Algemene Verordening Gegevensbescherming (AVG).

## 2.2 Uitbestedingsovereenkomst

In het uitbestedingsbeleid van een verzekeraar staan ook de voorwaarden waaraan de uitbestedingsovereenkomst behoren te voldoen. Voor de selectie van een dienstverlener, gaat de verzekeraar na aan welke wettelijke vereisten moet worden voldaan en legt deze vast, bijvoorbeeld in een model uitbestedingsovereenkomst.

Na, of zo mogelijk tijdens, het selecteren van een dienstverlener stelt een verzekeraar een (concept) contract op met de dienstverlener om de afspraken over de uit te besteden werkzaamheden vast te leggen. Zo'n contract geeft een waarborg dat de dienstverlener de werkzaamheden ook daadwerkelijk uitvoert conform de afspraken.

**Wettelijk kader**

Artikel 274.3C van de Solvency II verordeningen schrijft voor dat een verzekeraar de uitbestedingsovereenkomst schriftelijk vastlegt. Artikel 274.4 van de Solvency II Verordeningen stelt vervolgens welke elementen in ieder geval in dit contract aan bod komen.

## Artikel 274.4 – Solvency II Verordeningen 3015/35/EU

4. In de tussen de verzekerings- of herverzekeringsonderneming en de dienstverlener te sluiten schriftelijke overeenkomst als bedoeld in artikel 274 lid 3, onder c), worden met name alle volgende punten duidelijk vermeld:
   a. De taken en verantwoordelijkheden van beide betrokken partijen
   b. De toezegging van de dienstverlener dat hij zich zal houden aan alle toepasselijke wettelijke en bestuursrechtelijke voorschriften en richtsnoeren, alsook aan door de verzekerings- of herverzekeringsonderneming goedgekeurde gedragslijnen, en dat hij met betrekking tot de uitbestede functie of werkzaamheid met de toezichthoudende autoriteit van de onderneming zal samenwerken
   c. De verplichting van de dienstverlener om kennis te geven van elke ontwikkeling die van wezenlijke invloed kan zijn op zijn vermogen om de uitbestede functies en werkzaamheden efficiënt en met inachtneming van de toepasselijke wettelijke en bestuursrechtelijke voorschriften uit te voeren
   d. Een opzegtermijn voor de beëindiging van het contract door de dienstverlener welke lang genoeg is om de verzekerings- of herverzekeringsonderneming in staat te stellen een alternatieve oplossing te vinden
   e. Dat de verzekerings- of herverzekeringsonderneming de uitbestedingsovereenkomst indien nodig kan beëindigen zonder dat dit nadelige gevolgen heeft voor de continuïteit en de kwaliteit van haar dienstverlening aan verzekeringnemers
   f. Dat de verzekerings- of herverzekeringsonderneming zich het recht voorbehoudt te worden geïnformeerd over de uitbestede functies en werkzaamheden en over de uitvoering ervan door de dienstverlener, alsook het recht om de dienstverlener algemene richtsnoeren of individuele instructies te geven ten aanzien van datgene waarmee bij de uitvoering van de uitbestede functies of werkzaamheden rekening moet worden gehouden
   g. Dat de dienstverlener alle vertrouwelijke informatie over de verzekerings- of herverzekeringsonderneming en haar verzekeringnemers, begunstigden, werknemers, contractpartijen en alle andere personen moet beschermen
   h. Dat de verzekerings- of herverzekeringsonderneming, haar externe auditor en de toezichthoudende autoriteit effectief toegang moeten hebben tot alle informatie over uitbestede functies

en werkzaamheden, alsook tot de bedrijfsruimten van de dienstverlener om er controles ter plaatse te verrichten

i. Dat de toezichthoudende autoriteit, wanneer zulks voor toezichtdoeleinden passend en noodzakelijk is, rechtstreeks aan de dienstverlener vragen kan stellen, waarop de dienstverlener moet antwoorden.

j. Dat de verzekerings- of herverzekerings-onderneming informatie over de uitbestede werkzaamheden mag inwinnen en instructies mag geven met betrekking tot de uitbestede functies en werkzaamheden

k. De voorwaarden waaronder de dienstverlener eventueel enigerlei uitbestede functies en werkzaamheden verder mag uitbesteden

l. Dat de plichten en verantwoordelijkheden die uit hoofde van deze overeenkomst met de verzekerings- of herverzekerings-onderneming op de dienstverlener rusten, onverlet worden gelaten door een eventuele verdere uitbesteding in overeenstemming met punt k)

**Good practices**

Een verzekeraar sluit een uitbestedingsover-eenkomst (verder contract) af met een dienst-verlener met een duidelijke geldigheidsduur en herzieningsfrequentie. Het contract bevat een omschrijving van de uit te besteden activiteit en de voorwaarden waaronder de uitbesteding plaatsvindt, waaronder compliance met wet- en regelgeving.

Een verzekeraar legt in het contract een specificatie vast van de onderlinge informatie-uitwisseling en de controle- en rapportageverplichtingen van de dienstverlener, daaronder begrepen assuranceverklaringen en certificeringen. Onderdeel hiervan is de plicht tot informeren bij continuïteitsdreigingen of wijzigingen in eigendomsverhoudingen bij de dienstverlener.

Een verzekeraar legt in het contract redenen vast voor beëindiging van de overeenkomst, de wijze van transitie / migratie, de aansprakelijkheid en de inspanningsplicht van de dienstverlener hierbij. De verzekeraar streeft naar een zo ruim mogelijke bevoegdheid tot opzegging/ontbinding van de overeenkomst bij het niet handelen conform (kwaliteits)afspraken.

Een verzekeraar legt in het contract vast dat onderuitbesteding alleen is toegestaan als deze door uitbesteding niet aan het toezicht wordt onttrokken. De verzekeraar legt ook de condities en afspraken vast rondom onderuitbesteding, zoals de plicht dat de verzekeraar tijdig wordt geïnformeerd, zodat er voldoende tijd is om een risico-inschatting te maken en corrigerende maatregelen te kunnen nemen, alsook andere wettelijke vereisten die bij onderuitbesteding van toepassing zijn.

Bij onderuitbesteding neemt een verzekeraar passende maatregelen op in de contractvoorwaarden om het risico te mitigeren dat een onderaannemer niet in staat is om aan haar verplichtingen te voldoen.

Een verzekeraar neemt in het contract op dat de dienstverlener de verzekeraar in kennis stelt van alle voorgenomen belangrijke wijzigingen van de in de oorspronkelijke overeenkomst genoemde onderaannemers of in onderuitbesteding gegeven services. De kennisgevingstermijn voor dergelijke wijzigingen wordt zodanig bepaald dat de verzekeraar in staat is de risico's als gevolg van de voorgestelde wijziging te beoordelen en indien nodig corrigerende maatregelen kan nemen of de dienstverlener verlaten.

Het contract bevat bepalingen voor het right to examine (hierna onderzoeksrecht) voor de toezichthouders, het auditrecht voor de verzekeraar zelf en haar externe auditor. Bij mogelijkheden tot onderuitbesteding bevat het contract ook een raamovereenkomst, waarin dit is geregeld.

Een verzekeraar verplicht de hoofddienstverlener om het onderzoeksrecht voor DNB en het auditrecht voor de verzekeraar onvoorwaardelijk te regelen en deze rechten ook op te nemen in de contracten met de onderaannemers (hele keten). De feitelijke uitoefening van het onderzoeksrecht en het auditrecht zijn niet beperkt door contractuele regelingen. Dienstverleners verlenen effectieve toegang tot alle informatie over de uitbesteding en volledige toegang tot de bedrijfspanden (hoofdkantoor en operationele centra) met inbegrip van alle voorzieningen, systemen, netwerken en data die de dienstverlener gebruikt om de uitbestede diensten te leveren, zodat controles ter plaatse kunnen worden uitgevoerd.

Als een dienstverlener gevoelige data gaat verwerken sluit een verzekeraar een verwerkersovereenkomst af met de dienstverlener. In het verlengde maakt een verzekeraar afspraken over de eigendom van de data.

## 2.3 Kritieke en gevoelige data

Verzekeraars gaan voorzichtig om met kritieke en gevoelige data. Bij uitbesteding zorgen zij er voor dat de beschikbaarheid, integriteit, vertrouwelijkheid en beveiliging van hun kritieke en gevoelige data is gewaarborgd.

**Wettelijk kader**

Artikel 274.3(e) van de Solvency II Verordeningen stelt dat uitbesteding geen inbreuk mag hebben op enigerlei wet- en regelgeving, daaronder begrepen de Algemene Verordening Gegevensbescherming (AVG). Wanneer bij de verzekeraar voor bepaalde gegevens beleid geldt inzake beschikbaarheid, integriteit en vertrouwelijkheid (informatiebeveiligings- en BCM beleid), waarborgen de dienstverlener en haar onderaannemers, de veiligheid van de gegevens op minimaal gelijkwaardig of hoger niveau, zo volgt uit artikel 274.3(f) van de Solvency II Verordeningen. De verzekeraar zorgt er zelf voor dat zij en de dienstverleners waaraan is uitbesteed voldoen aan de vereisten ten aanzien van informatiebeveiliging, zie ook Open Boek Toezicht.

## Artikel 274.3 – Solvency II Verordeningen 3015/35/EU

3. Bij de keuze van de in lid 1 bedoelde dienstverlener voor kritieke of belangrijke operationele functies of werkzaamheden, zorgt het bestuurlijk, beleidsbepalend of toezichthoudend orgaan voor het volgende:
   e. De uitbesteding heeft geen inbreuk op enigerlei wet, en met name de regelgeving inzake gegevensbescherming
   f. De dienstverlener is aan dezelfde voorschriften inzake de veiligheid en de vertrouwelijkheid van informatie betreffende de verzekerings- of herverzekeringsonderneming of de verzekeringnemers of begunstigden daarvan onderworpen als die welke voor de verzekerings- of herverzekeringsonderneming gelden.

**Good practices**

Een verzekeraar definieert en neemt besluiten over passende bescherming voor de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. Een verzekeraar gaat na of specifieke maatregelen nodig zijn voor gegevens in transport, gegevens in bewerking en gegevens in opslag (productie en back-up), zoals de toepassing van sterke authenticatie en versleuteltechnieken (encryptie) in combinatie met een passende opzet voor het management van het sleutelbeheer. De verzekeraar monitort de getroffen maatregelen met inbegrip van incidenten.

Een verzekeraar bewaakt (voortdurend) de toegang van de dienstverlener tot kritieke en gevoelige data, bijvoorbeeld aan de hand van beveiligingslogs of andere controlemiddelen.

Een verzekeraar is voorzichtig met het aangaan en beheren van contracten buiten de Europese Economische Ruimte (EER) vanwege risico's die kunnen samengaan met de plaats van de gegevens en de gegevensverwerking. De verzekeraar beoordeelt en adresseert mogelijke gevolgen van risico's, inclusief beperkingen voor het toezicht in verband met de landen waar de gegevens worden opgeslagen.

Een verzekeraar is naar de betrokkenen transparant over de uitbesteding en verstrekking van persoonsgegevens aan derde partijen.

Een verzekeraar zorgt er voor dat de rechten van betrokkenen niet beperkt of gehinderd worden.

Een verzekeraar is in staat om de naleving van de AVG door de dienstverlener vast te stellen. Het niet naleven van de AVG en de gemaakt afspraken, kan voor een verzekeraar aanleiding zijn tot het beëindigen van de overeenkomst met de dienstverlener

# 3. Selectieproces



Nadat een verzekeraar heeft vastgesteld welke werkzaamheden zij wil uitbesteden en aan welke wettelijke vereisten er moet worden voldaan, gaat zij op zoek naar een dienstverlener die de betreffende werkzaamheden voor de verzekeraar kan uitvoeren. De verzekeraar gaat na of de dienstverlener aan zowel alle eisen uit de wet- en regelgeving als aan het beleid en de eisen en wensen van de verzekeraar voldoet.

## 3.1 Selectie dienstverlener

Vanuit het wettelijk volgt dat de potentiele dienstverlener de werkzaamheden moet kunnen uitvoeren, en er moet een proces zijn waarmee die selectie van een bekwame dienstverlener wordt geborgd.

### 274.3 – Solvency II verordeningen 3015/35/EU

3. Bij de keuze van de in lid 1 bedoelde dienstverlener voor kritieke of belangrijke operationele functies of werkzaamheden, zorgt het bestuurlijk, beleidsbepalend of toezichthoudend orgaan voor het volgende:
   a. Er wordt diepgaand onderzoek verricht om te waarborgen dat de potentiële dienstverlener over de bekwaamheid, de capaciteit en elke bij wet vereiste vergunning beschikt om de vereiste functies of werkzaamheden op bevredigende wijze uit te voeren, rekening houdend met de doelstellingen en behoeften van de onderneming
   b. De dienstverlener heeft al het nodige gedaan om te voorkomen dat daadwerkelijke of potentiële belangenconflicten de behoeften van de uitbestedende onderneming doorkruisen

### Artikel 274.5 - Solvency II verordeningen 3015/35/EU

De verzekerings- of herverzekeringsonderneming die kritieke of belangrijke operationele functies of werkzaamheden uitbesteedt, voldoet aan alle volgende vereisten:

c. Zij verifieert of de dienstverlener over de vereiste financiële draagkracht beschikt om de extra taken op behoorlijke en betrouwbare wijze te vervullen, en of alle medewerkers van de dienstverlener die bij de uitvoering van de uitbestede functies of werkzaamheden betrokken zullen zijn, voldoende gekwalificeerd en betrouwbaar zijn

## Richtsnoer 63 – Schriftelijke beleidslijn inzake uitbesteding

1.116 De onderneming die activiteiten of functies uitbesteedt of die voornemens is om dat te gaan doen, moet in haar beleidslijn inzake uitbesteding de aanpak en processen die van toepassing zijn op de uitbesteding bestrijken en wel gedurende de volledige looptijd van de betreffende overeenkomst. In dat beleid moet met name aandacht worden besteed aan de volgende aspecten:

b. De wijze waarop een dienstverlener van een adequaat kwaliteitsniveau wordt geselecteerd en hoe en met welke frequentie de prestaties en resultaten van de dienstverlener worden beoordeeld

**Good practices**

Aan de selectie van een dienstverlener gaat een risicoanalyse vooraf die ook concentratierisico op de dienstverlener, juridisch risico en een due diligence beoordeling omvat. Daarbij houdt de verzekeraar rekening met risico's die uit diverse scenario's voortkomen, zoals een situatie waarin de dienstverlener niet tot nakoming in staat is, buitenlandse activiteiten, concurrentie, groei, verlies van kennis binnen de verzekeraar etc.

In het selectieproces van een dienstverlener komen onder andere de volgende aspecten aan bod:

- financiële situatie van de dienstverlener en mogelijke belangenverstrengeling
- professionele achtergrond en expertise van de medewerkers van de dienstverlener
- screening van medewerkers (antecedenten-onderzoek)
- omvang van de opdracht in relatie tot de omvang van de dienstverlener
- geschillen of gerechtelijke procedures waarbij de dienstverlener is betrokken
- reputatie van de dienstverlener
- kwaliteit van onderaannemers
- standaardcertificeringen, audit- en assurance-rapporten
- informatiebeveiligingsbeleid van de dienst-verlener
- continuïteitsbeleid van de dienstverlener
- compliancebeleid van de dienstverlener
- privacybeleid
- incidentrapportage beleid van de dienstverlener
- toepasselijke recht en land van vestiging van de dienstverlener
- veiligheid van de gegevens
- locatie van data-opslag, indien van toepassing
- waarborgen voor uitoefening van toezicht

Het selectieproces van een verzekeraar kent processtappen, selectiecriteria en een besluitvormingsproces dat leidt tot duidelijke mandaten voor de dienstverlener met de directie van een verzekeraar als eindverantwoordelijke. Op basis van de selectiecriteria vraagt de verzekeraar dienstverleners informatie aan te leveren zodat een 'longlist' ontstaat. De lijst van potentiële dienstverleners wordt terug gebracht tot een 'shortlist' op basis van de uitkomsten van de onderzochte aspecten. De verzekeraar start de contractonderhandelingen met geschikte dienstverleners waarvan het risicoprofiel past bij de risicobereidheid van de verzekeraar. In het geval

geen geschikte dienstverlener wordt gevonden, houdt de verzekeraar de uitgangspunten en selectiecriteria opnieuw tegen het licht en stelt zichzelf de vraag of uitbesteding in dit geval een goede optie is.

Een verzekeraar laat de juridische aspecten van uitbestedingscontracten toetsen voordat de verzekeraar de contracten ondertekent. Een verzekeraar gaat na of er geen contraproductieve of conflicterende afspraken zijn gemaakt.
De overeenkomst wordt op het hoogste managementniveau ondertekend.

# 4. Monitoring

Na het aangaan van een contract houdt de verzekeraar in de gaten of de dienstverlener ook daadwerkelijk de services levert die de verzekeraar met de dienstverlener heeft afgesproken. De verzekeraar monitort de uitvoering van de activiteiten, de effectiviteit van de getroffen beveiligings- en controlemaatregelen en gaat na of aan wet- en regelgeving wordt voldaan. De verzekeraar treft waar nodig onmiddellijk corrigerende maatregelen.

## 4.1 Monitoring uitbesteding

Een verzekeraar past intern haar processen aan om de uitbesteding te monitoren en beschikt daarbij over toereikende procedures, maatregelen, deskundigheid en informatie.

### Wettelijk kader

**Artikel 274.5 - Solvency II verordeningen 3015/35/EU**

De verzekerings- of herverzekeringsonderneming die kritieke of belangrijke operationele functies of werkzaamheden uitbesteedt, voldoet aan alle volgende vereisten:

a. Zij zorgt ervoor dat de relevante aspecten van het risicomanagement- en interne controlesysteem van de dienstverlener adequaat genoeg zijn om de naleving van artikel 49, lid 2, onder a) en b), van Richtlijn 2009/138/EG te waarborgen
b. Zij houdt in haar risicomanagement- en interne controlesysteem afdoende rekening met de uitbestede werkzaamheden om de naleving van artikel 49, lid 2, onder a) en b), van Richtlijn 2009/138/EG te waarborgen

### Good practices

De directie van een verzekeraar houdt in haar risicomanagement- en interne controlesysteem rekening met de uitbestede activiteiten om de uitvoering te kunnen beoordelen en naleving van wet- en regelgeving te waarborgen. Op regelmatige basis afhankelijk van de controlemaatregel controleert een verzekeraar de aantoonbare werking van interne controle maatregelen van de aan uitbesteden verbonden risico's en rapporteert de bevindingen hiervan aan de directie.

De verzekeraar bewaakt de met de uitbesteding gepaard gaande risico's, waaronder operationele- en concentratierisico's, doorlopend en vergelijkt de informatie van de dienstverlener met vastgelegde kritieke risico indicatoren (KRI's) voor uitbestedingsrisico's zodat de verzekeraar veranderingen in het risicoprofiel tijdig herkent. Voorbeelden van kritieke risico indicatoren zijn:

- aantal verstoringen met direct operationeel effect op de dienstverlening of de verwachte inkomsten
- aantal klachten van polishouders
- aantal data-incidenten
- mate van compliance aan wet- en regelgeving
- mate van effectieve werking (%) van interne controle maatregelen van uitbestedingsrisico's
- concentraties op dienstverleners

Een verzekeraar heeft voor het monitoren van grotere uitbestedingen een regieorganisatie die passend is bij de aard, omvang en complexiteit van zowel de verzekeraar als de uitbestede activiteiten.

Een verzekeraar richt monitoring in ten aanzien van de werking en effectiviteit van de controlemaatregelen van de dienstverlener. Daarnaast is de monitoring van de verzekeraar gericht op het tijdig verzamelen van gegevens die een indicatie kunnen zijn van een verminderde prestatie of continuïteit.

Een verzekeraar beschrijft de benodigde kennis en competenties om de dienstverlener tegenwicht te geven (zie onderdeel 1, beleid). De verzekeraar beschrijft ook de specifieke competenties die nodig zijn om KPI rapportages goed te kunnen beoordelen. Dit geldt ook voor het beoordelen van service level rapportages (4.2) en assurancerapportages (4.3).

De risicomanagementfunctie verzamelt, aggregeert en rapporteert de informatie over de uitbestedingen minimaal per kwartaal en rapporteert hierover aan de directie. Aan de hand van deze informatie is de directie in staat de operationele risico's verbonden aan alle uitbestede werkzaamheden op effectieve wijze te beheersen.

Een verzekeraar heeft volledig zicht op de ketens van uitbesteding. De monitoringrapportages beslaan de gehele scope van de afgenomen diensten. De verzekeraar ontvangt op reguliere basis rechtstreeks van de onderaannemer of via de 'hoofddienstverlener' informatie over onderuitbestedingen. Afhankelijk van de materialiteit van de afgenomen service zijn dit incidentenrapportages, service level rapportages en assurancerapportages over de kwaliteit van de dienstverlening en de effectiviteit van de interne beheersingsmaatregelen.

Een verzekeraar houdt een centrale registratie bij met informatie van de activiteiten die zij uitbesteedt. Dit register bevat de gegevens van alle uitbestedingsrelaties inclusief relevante onderuitbestedingen. De verzekeraar houdt in het register de volgende informatie bij van de dienstverleners:

- NAW gegevens van dienstverleners en hun onderaannemers, indien van toepassing
- KVK gegevens
- Beschrijving van de uitbesteding
- Start- en einddatum of de eerstvolgende datum van verlenging van de overeenkomst
- Toepasselijk recht van de overeenkomst
- Land of de landen waar de dienst wordt verleend met indien van toepassing de plaats van de gegevens
- Uitkomst en datum van de materialiteits-beoordeling
- Eigen classificatie op gebied van beschikbaarheid, integriteit en vertrouwelijkheid (BIV)
- Bewijs van goedkeuring door hoogste managementniveau om te borgen dat de uitbesteding aan de wettelijke eisen én de eigen selectiecriteria voldoet
- Beoordeling of er een alternatieve dienstverlener is in termen van eenvoudig, moeilijk, onmogelijk en zo ja, gegevens van deze dienstverlener
- Datum laatste evaluatie van de dienstverlener
- Datum laatste verlenging van de overeenkomst (indien van toepassing)

## 4.2 Service level rapportages (SLR)

Een verzekeraar ontvangt rapportages over de performance van de dienstverlener. Deze rapportages stellen een verzekeraar in staat om de kwaliteit van de uitbesteding te monitoren en de uitbestedingsrisico's te beheersen.

### Wettelijke kader

Artikel 258(1h,i,k) van de Solvency II Verordeningen met algemene governance vereisten stelt dat een verzekeraar informatiesystemen en rapportagelijnen opzet die passende en overzichtelijke gegevens over de interne organisatie en informatie over de risico's tijdig bij de juiste personen bekend maken.

### Good practices

In een Service Level Agreement (SLA) legt een verzekeraar afspraken vast over de overeengekomen prestaties tussen de verzekeraar en de dienstverlener, inclusief de wederzijdse verantwoordelijkheden aansluitend op het uitbestedingscontract. Daarbij legt de verzekeraar detailwerkafspraken vast in een Document Afspraken en Processen (verder DAP). Dit bevat onder meer:

- Contactpersonen
- Hoe te bereiken
- Hoe wijzigingen aan te leveren
- Geagendeerde afspraken en frequentie
- Operationeel, tactisch en strategisch overleg.
- Oplossen van geschillen
- Escalatieprocedure

In de SLA ligt vast hoe de dienstverlener vorm geeft aan de uitvoering van het contract en hoe het prestatiemanagement plaatsvindt: prestatie-indicatoren, meting, periodiciteit, normering (tolerantiegrenzen). Een verzekeraar maakt afspraken over onder meer de volgende prestatie-indicatoren en bepaalt een norm die niet mag worden overschreden:

- Openstellingstijden
- Beschikbaarheid (%)
- Aantallen en aard incidenten: security, cybercrime, data-issues
- Reactietijd op incidenten
- Oplostijd incidenten
- Gebruikersondersteuning
- Klachten
- Probleemherstel en onderhoudsronden
- Beveiligingsniveau: omgang gevoelige data, opleiding en instructie
- Aantallen gebruikers
- Aantallen transacties
- Achterstanden
- Levertermijn

Een verzekeraar vergewist zich dat de uitbestede services blijvend voldoen aan de afgesproken prestatie- en kwaliteitsnormen aan de hand van vooraf overeen gekomen service level rapportages waarin wordt gerapporteerd over de afgesproken prestatie-indicatoren.

Een verzekeraar laat de kritieke performance indicatoren (KPI's) in de SLA aansluiten bij de doelen uit het uitbestedingsbeleid. Ook de risicobereidheid van de verzekeraar sluit aan bij de gehanteerde kritieke risico indicatoren (KRI's).

Een verzekeraar bewaakt en beoordeelt of de service toereikend is, zodat de verzekeraar de dienstverlener tijdig de benodigde herstelmaatregelen kan laten nemen als dat nodig is. Voor een dergelijke beoordeling maakt de verzekeraar gebruik van een combinatie van kwantitatieve en kwalitatieve indicatoren die gebaseerd zijn op recente operationele gegevens van de dienstverlener.

Afspraken over rapportagemomenten passen bij aard en omvang van de uitbesteding; minimaal per kwartaal, per maand of doorlopend op basis van tooling waarin de verzekeraar en de dienstverlener samenwerken. De SLA en/of de DAP bevat afspraken over informatie-uitwisseling, controles, Service Level Rapporten (SLR), periodiek overleg en een klachten- en incidentenproces inclusief rapportagemomenten en normen.

## 4.3 Assurance over de kwaliteit van de uitbestede diensten

Een verzekeraar ontvangt rapportages over de dienstverlener, zowel van de dienstverlener zelf als van onafhankelijke derden (third party). Deze rapportages stellen een verzekeraar in staat om de kwaliteit van de uitbesteding te monitoren en de uitbestedingsrisico's te beheersen.

**Good practices**

In het uitbestedingscontract met de dienstverlener maakt de verzekeraar afspraken dat de dienstverlener regelmatig assurance levert over het stelsel van haar interne beheersing. Dit kan op basis van een assurancerapportage opgesteld door een onafhankelijke 'assuranceprovider' (third party) of op basis van een audit die de verzekeraar bij de dienstverlener uitvoert of laat uitvoeren.

Een verzekeraar zorgt er voor dat de scope van de ontvangen assurance en de periode waarover deze assurance is afgegeven, aansluit bij de afgenomen dienstverlening. De verzekeraar kiest voor een assuranceverklaring over opzet, bestaan en aantoonbare werking over een bepaalde periode.

Voor ICT dienstverlening kiest een verzekeraar voor een SOC2 en/of SOC3 verklaring. Voor verantwoording over uitbestede dienstverlening in het kader van de jaarrekening, kiest een verzekeraar voor een ISAE3402 type II of SOC1 verklaring.
De ontvangen assurance heeft betrekking op de kwaliteit van de dienstverlening met betrekking tot de gehele keten. De verzekeraar ontvangt de assurance geaggregeerd van de hoofduitvoerder of van alle betrokken dienstverleners afzonderlijk.
De verzekeraar monitort de opvolging van bevindingen uit de assurancerapportages actief.
De verzekeraar weegt de bevindingen, matcht deze met de eigen waarnemingen en klachten- en incidentenrapportages. De verzekeraar maakt een risico-inschatting, stuurt zonodig bij en legt dit vast

Een verzekeraar zorgt er voor dat er voldoende kennis en expertise beschikbaar is, bijvoorbeeld een multidisciplinair team, om de assurancerapportage te beoordelen.

Een verzekeraar voert eigen audits uit bij dienstverleners als alternatief voor het ontbreken

van een assuranceverklaring of als aanvulling op een assuranceverklaring die onvoldoende aansluit bij de afgenomen dienstverlening.

Bij de evaluatie van een assuranceverklaring let een verzekeraar er op dat de aan haar geleverde dienstverlening in de reikwijdte van de rapportage is opgenomen en ook in de steekproef.

De (controlerend) accountant stelt een juiste, volledige en tijdige werking van de controles vast op basis van een representatieve steekproef. Indien nodig voert een verzekeraar aanvullend eigen audit onderzoek uit.

Een verzekeraar die niet beschikt over voldoende eigen auditmiddelen kan samen met andere klanten van dezelfde (cloud) dienstverlener een audit organiseren. Op deze manier zetten deze partijen hun auditmiddelen efficiënter in en blijven de organisatorische lasten voor de dienstverlener ook meer beperkt. Cloudoplossingen zijn technisch bijzonder complex. Vooraf verifieert de verzekeraar dat de auditor die de audit verricht, beschikt over de juiste kennis en vaardigheden om audits en/of beoordelingen van cloudoplossingen op een doeltreffende wijze uit te voeren.

Een verzekeraar onderkent de mogelijkheden en beperkingen van de verschillende vormen van assurance en (ISO-)certificeringen. Een certificering richt zich op de kwaliteit van de opzet van processen op enig moment. Een verzekeraar neemt waar nodig maatregelen om de gewenste bevestiging over het functioneren van processen te verkrijgen.

# 5. Evaluatieproces



Na verloop van tijd doet een verzekeraar meer ervaring op met de processen rond de uitbestede werkzaamheden en de kwaliteit van de dienstverleners. Op gezette tijden, of zoveel eerder als daar aanleiding toe is, evalueert de verzekeraar het functioneren van de dienstverleners die werkzaamheden verrichten voor de verzekeraars.

**Wettelijk kader**

Artikel 41 van de Richtlijn en artikel 258.6 van de Solvency II Verordeningen schrijft voor dat de verzekeraars op gezette tijden hun governancesysteem, hieronder begrepen de uitbestedingen, evalueren. Richtsnoer 63 van de EIOPA Richtsnoeren over het governancesysteem vraagt aandacht voor de wijze waarop en met welke frequentie de dienstverlener wordt beoordeeld.

## Artikel 41 - Algemene governancevereisten Richtlijn 2009/138/EG

1. De lidstaten schrijven voor dat alle verzekerings- en herverzekeringsondernemingen moeten beschikken over een doeltreffend governancesysteem dat voor een gezonde en prudente bedrijfsvoering zorgt. Dit systeem bevat in elk geval een adequate transparante organisatiestructuur met een duidelijke verdeling en correcte scheiding van verantwoordelijkheden en een doeltreffend systeem voor de overdracht van informatie. Ook zorgt het ervoor dat de artikelen 42 tot en met 49 worden nageleefd. Het governancesysteem wordt intern periodiek geëvalueerd.
2. Het governancesysteem is proportioneel aan de aard, omvang en complexiteit van de verrichtingen van de verzekerings- of herverzekeringsonderneming.
3. Verzekerings- en herverzekeringsondernemingen beschikken in elk geval voor het riskmanagement, de interne controle, de interne audit en indien van toepassing, voor uitbestedingen over schriftelijk vastgelegde beleidslijnen. Zij zorgen ervoor dat deze beleidslijnen worden toegepast. Deze schriftelijk vastgelegde beleidslijnen worden ten minste eenmaal per jaar geëvalueerd. Ze worden vooraf door het bestuurlijk, beleidsbepalend of toezichthoudend orgaan goedgekeurd en ze worden aangepast bij een duidelijke wijziging van het betrokken systeem of gebied.

## Artikel 258 - Algemene governance vereisten Solvency II Verordeningen 3015/35/EU

6. Verzekerings- en herverzekeringsondernemingen monitoren en evalueren op gezette tijden de deugdelijkheid en doeltreffendheid van hun governancesysteem en nemen passende maatregelen om eventuele onvolkomenheden te verhelpen.

### Richtsnoer 63 – Schriftelijke beleidslijn inzake uitbesteding

1.116 De onderneming die activiteiten of functies uitbesteedt of die voornemens is om dat te gaan doen, moet in haar beleidslijn inzake uitbesteding de aanpak en processen die van toepassing zijn op de uitbesteding bestrijken en wel gedurende de volledige looptijd van de betreffende overeenkomst. In dat beleid moet met name aandacht worden besteed aan de volgende aspecten:

e. De wijze waarop een dienstverlener van een adequaat kwaliteitsniveau wordt geselecteerd en hoe en met welke frequentie de prestaties en resultaten van de dienstverlener worden beoordeeld

## 5.1 Evaluatie in alle stappen van het uitbestedingsproces

Een verzekeraar evalueert niet alleen de dienstverleners waaraan zij werkzaamheden uitbesteedt, maar ook het eigen uitbestedingsbeleid (zie 1) en de uitbestedingsprocessen: selectie (3), monitoring (4) en evaluatie (5). Zijn de interne rapportagelijnen bijvoorbeeld goed ingericht om tijdig op de hoogte te zijn van incidenten bij dienstverleners, sluiten processen en controles nog aan op het beleid en voldoet de standaard voor uitbestedingsovereenkomsten nog aan de huidige wet- en regelgeving en de laatste ontwikkelingen?

**Good practice**

Een verzekeraar evalueert periodiek maar minimaal jaarlijks het beleid. De verzekeraar documenteert de uitkomst hiervan en informeert het juiste managementniveau over afwijkingen en mogelijke corrigerende maatregelen. Op basis van de evaluatie past de verzekeraar het uitbestedingsbeleid indien nodig aan en gaat de verzekeraar na of door aanpassing van het beleid de bestaande uitbestedingen moeten worden bijgesteld of beëindigd.

## 5.2 Evaluatie dienstverleners

Op gezette tijden evalueert een verzekeraar de dienstverleners, of zoveel eerder als uit de monitoring signalen van slecht functioneren naar voren komen. Daarnaast evalueert de verzekeraar of de uitbestedingen nog in het strategisch beleid en de risicobereidheid van de verzekeraar passen.

**Good practices**

Gedurende de looptijd van de overeenkomst evalueert de verzekeraar de dienstverlener met een in het beleid vastgestelde aanpak en frequentie. Materiële uitbestedingen evalueert de verzekeraar minimaal jaarlijks. Daarbij gaat het onder andere om het behalen van de gemaakte performance- en resultaatafspraken en het evalueren van grote wijzigingen die zich bij de dienstverlener voordoen, zoals wijzigingen in de strategie, de winstgevendheid, de eigendomsverhoudingen of andere aspecten die invloed hebben op de mate waarin de dienstverlener aan de contractverplichtingen kan voldoen.

De evaluatie leidt tot een besluit op het juiste managementniveau om de uitbesteding te continueren, bij te stellen of te beëindigen. De vraag die hierbij centraal staat is: willen we bij de huidige dienstverlener blijven of gaan we verder de markt verkennen op zoek naar een andere dienstverlener die beter past bij de missie, visie en strategie van de verzekeraar.

Een verzekeraar wijst organisatie-eenheden of personen aan die verantwoordelijk zijn voor de controle, het beheer en de evaluatie van de uitbesteding. De verzekeraar geeft hierbij de voorkeur aan realisatie in multidisciplinair verband.

Een verzekeraar toetst de oorspronkelijke business case van uitbesteding aan haar beleid.

Een verzekeraar evalueert haar eigen beleid in het licht van de uitkomsten van de evaluatie van de dienstverleners. Dit kan tot aanpassing van het beleid leiden.

In de evaluatie gaat een verzekeraar na of de uitbesteding nog aan de eisen voldoet, aansluit bij de risicobereidheid en bijdraagt aan het behalen van haar doelstellingen. Onder andere de volgende aspecten maken standaard deel uit van de evaluatie:

- financiële situatie van de dienstverlener en mogelijke belangenverstrengeling
- professionele achtergrond en expertise van de medewerkers van de dienstverlener
- omvang van de opdracht in relatie tot de omvang van de dienstverlener
- geschillen of gerechtelijke procedures waarbij de dienstverlener is betrokken
- reputatie van de dienstverlener
- kwaliteit van onderaannemers
- monitoringsmechanismen
- standaardcertificeringen, audit- en assurancerapporten
- informatiebeveiligingsbeleid van de dienstverlener
- continuïteitsbeleid van de dienstverlener
- compliancebeleid van de dienstverlener
- incidentrapportage beleid van de dienstverlener
- locatie van de gegevens, indien van toepassing

**DISCLAIMER**

Deze Good Practice geeft niet-verplichtende aanbevelingen aan verzekeraars voor de toepassing van de Solvency II Richtlijn en Verordeningen, de Wet op het financieel toezicht, het Besluit prudentiële regels en EIOPA Richtsnoeren waar deze betrekking hebben op risicomanagement. Met behulp van deze Good Practice draagt de Nederlandsche Bank N.V. haar opvattingen uit over de door haar geconstateerde of verwachte gedragingen in de beleidspraktijk, die naar haar oordeel een goede toepassing inhouden van de regels waarop deze Good Practice betrekking heeft.

Met deze Good Practice beoogt de Nederlandsche bank N.V. te bereiken dat verzekeraars het daarin gestelde, de eigen omstandigheden in aanmerking nemende, in hun afweging betrekken, zonder dat zij verplicht zijn dat te doen. De Good Practice geeft inzicht in de door DNB geconstateerde of te verwachten gedraging in de beleidspraktijk, is indicatief van aard en sluit daarmee niet uit dat voor instellingen een afwijkend, al dan niet strengere toepassing van de onderliggende regels geboden is. De afweging betreffende de toepassing berust bij deze instellingen zelf.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl