Datakwaliteit beleid

InRisk Schadeverzekeringen NV

Leuvenheim,
15 maart 2018

VERSIEBEHEER

Versie	Datum	Wijzigingen	Auteur
0.1	__/__/18	Eerste concept document	InRisk
0.9	__/__/18		…
1.0	__/__/18		…

Verantwoordelijk

Naam	Afdeling
Ronald van de Langenberg	CFRO InRisk Schadeverzekeringen NV

Afgestemd met

Naam	Afdeling
Abc	ABC
Abc	ABC
Abc	ABC
Abc	ABC
Abc	ABC
Abc	ABC
Abc	ABC

Gerelateerde beleidsdocumenten

Beleidsdocumenten

Inhoudsopgave

Doelstelling van het datakwaliteit beleid

Dit datakwaliteit beleid is opgesteld om te voldoen aan het vereiste in artikel 55, 82 en 86f van de Solvency II Directive (2009/138), uitgewerkt in EIOPA Richtsnoer EIOPA-BoS-14/166 – Richtsnoeren voor de waardering van technische voorzieningen.

De nadruk in dit document ligt op het definiëren van de interne vereisten die gesteld worden aan de kwaliteit van de data die de grondslag vormt voor het berekenen van technische voorzieningen, maar ook aan andere te gebruiken data. De vereisten aan de financiële rapportage kunnen worden gevonden in het rapportagebeleid.

De Solvency II wet- en regelgeving vereisen een beleidsraamwerk voor de datakwaliteit. Met dit document voldoen wij daaraan. Dit document strekt zich naast de vereisten voor de Solvency II regelgeving ook uit over de overige datakwaliteit binnen onze onderneming.

Tenslotte heeft DNB op 1 september 2017 een Guidance document ('Guidance beheersing Solvency II datakwaliteit door verzekeraars') uitgebracht waarin zij nadere invulling geeft aan haar verwachtingen omtrent de beheersing van datakwaliteit.

Definitie datakwaliteit

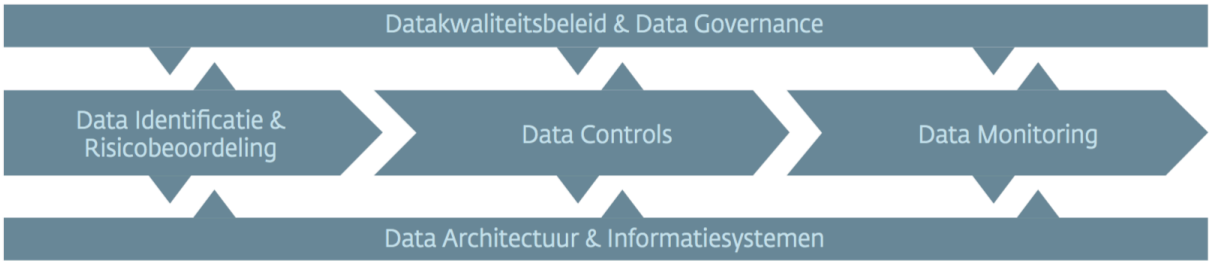
Datakwaliteit wordt gemeten in termen van adequaatheid, volledigheid en juistheid. Dit datakwaliteit beleid beschrijft de standaarden voor het vereiste niveau van datakwaliteit.

Datakwaliteit moet ook aantoonbaar zijn. Dit beleid schrijft voor hoe dit niveau wordt bereikt, wordt bewaakt en hoe hierover wordt gerapporteerd.

Tevens beschrijft dit beleid de adequate governance, en effectieve controles in juiste verhouding tot de aard, omvang en complexiteit van de dataprocessen.

Elementen van het management van datakwaliteit

In het Guidance document van DNB zijn de elementen van datakwaliteitsmanagement als onderstaand geschetst. Deze indeling is ook voor deze verzekeraar goed toepasbaar:



Onder het hoofdstuk 'Processen en controls' wordt dit schema voor deze verzekeraar nader uitgewerkt.

Normenkader

Datakwaliteit wordt gemeten in termen van adequaatheid, volledigheid en juistheid. Daarom zal deze documentatie standaarden beschrijven voor het vereiste niveau van datakwaliteit, en hoe dit niveau bereikt wordt. Tevens beschrijft het de adequate governance, en effectieve controles die in de juiste verhouding staan tot de schaal en complexiteit van de dataprocessen.

Relevante regelgeving

Artikel 55 van de Solvency II Richtlijn
Dit artikel schrijft voor dast de verzekeringsondernemingen over passende systemen en structuren moeten beschikken om aan de vereisten van de wet te voldoen, en over een schriftelijk vastgelegde gedragslijn die waarborgt dat de bekendgemaakte informatie altijd correct is. Dit artikel strekt zich derhalve ook uit over de data en de modellen waarmee technische voorzieningen worden berekend.

Artikel 48, 1c van de Solvency II Richtlijn
De kwaliteit van de data die gebruikt worden voor de berekening van de technische voorzieningen vereisen extra aandacht vanwege de mogelijke impact van inadequate, onvolledige of onjuiste data. Daarom is de beoordeling van deze datakwaliteit belegd bij de actuariële functie, die “beoordeelt of genoeg gegevens worden gebruikt bij de berekening van technische voorzieningen, en zij beoordeelt de kwaliteit ervan.”

Artikel 82 van de Solvency II Richtlijn
“Verzekeringsondernemingen beschikken over interne processen en procedures om de adequaatheid, volledigheid en juistheid te waarborgen van de gegevens waarvan gebruik wordt gemaakt bij de berekening van hun technische voorzieningen”.

Artikel 86f van de Solvency II Richtlijn
De commissie stelt gedelegeerde handelingen vast ter bepaling van het volgende […]
f. de normen waaraan moet worden voldaan om de adequaatheid, volledigheid en juistheid te waarborgen van de gegevens die bij de berekening voor de technische voorzieningen worden gebruikt […].
De gedelegeerde handelingen zijn gepubliceerd onder nummer 2015/35.

Artikel 19 van de Gedelegeerde handelingen 2015/35
Bij de berekening van de technische voorzieningen gebruikte gegevens

1. De bij de berekening van de technische voorzieningen gebruikte gegevens worden pas als volledig in de zin van artikel 82 van Richtlijn 2009/138/EG aangemerkt wanneer aan alle volgende voorwaarden is voldaan:

> *(a) de gegevens bevatten voldoende historische informatie om de kenmerken van de onderliggende risico's te beoordelen en om trends in de risico's te onderkennen;*
>
> *(b) de gegevens zijn beschikbaar voor elk van de relevante homogene risicogroepen waarvan bij de berekening van de technische voorzieningen wordt gebruikgemaakt en er worden geen relevante gegevens zonder motivering buiten beschouwing gelaten bij de berekening van de technische voorzieningen.*

2. De bij de berekening van de technische voorzieningen gebruikte gegevens worden pas als juist in de zin van artikel 82 van Richtlijn 2009/138/EG aangemerkt wanneer aan alle volgende voorwaarden is voldaan:

> *(a) de gegevens bevatten geen materiële fouten;*
>
> *(b) de voor dezelfde schatting gebruikte gegevens van verschillende perioden zijn consistent;*
>
> *(c) de gegevens worden tijdig en consistent in de tijd geregistreerd.*

3. De bij de berekening van de technische voorzieningen gebruikte gegevens worden pas als adequaat in de zin van artikel 82 van Richtlijn 2009/138/EG aangemerkt wanneer aan alle volgende voorwaarden is voldaan:

(a) de gegevens beantwoorden aan de doelen waarvoor zij zullen worden gebruikt;

(b) de omvang en de aard van de gegevens garanderen dat de schattingen die bij de berekening van de technische voorzieningen op basis van de gegevens worden gemaakt, geen materiële schattingsfout bevatten;

(c) de gegevens zijn consistent met de aannamen die ten grondslag liggen aan de actuariële en statistische methoden die bij de berekening van de technische voorzieningen daarop worden toegepast;

(d) de gegevens weerspiegelen op adequate wijze de risico's waaraan de verzekerings- of herverzekeringsonderneming in verband met haar verzekerings- en herverzekeringsverplichtingen is blootgesteld;

(e) de gegevens zijn op transparante en gestructureerde wijze verzameld, verwerkt en toegepast volgens een gedocumenteerd proces dat alle volgende elementen omvat:

i) de vaststelling van criteria voor de gegevenskwaliteit en een beoordeling van de gegevenskwaliteit, met inbegrip van specifieke kwalitatieve en kwantitatieve normen voor verschillende gegevensbestanden;

ii) het gebruiken en maken van aannamen bij de verzameling, verwerking en toepassing van gegevens;

iii) het proces voor het verrichten van actualiseringen van gegevens, met inbegrip van de frequentie van actualiseringen en de omstandigheden die tot extra actualiseringen aanleiding geven;

(f) verzekerings- en herverzekeringsondernemingen dragen er zorg voor dat hun gegevens op consistente wijze in de tijd worden gebruikt bij de berekening van de technische voorzieningen.

Voor de toepassing van punt b) wordt een schattingsfout bij de berekening van de technische voorzieningen als materieel aangemerkt wanneer deze de besluitvorming of het oordeel van de gebruikers van de uitkomst van de berekening, met inbegrip van de toezichthoudende autoriteiten, kan beïnvloeden.

4. Verzekerings- en herverzekeringsondernemingen mogen gebruikmaken van gegevens die uit een externe bron afkomstig zijn, op voorwaarde dat zowel aan de vereisten van de leden 1 tot en met 4 als aan alle volgende vereisten is voldaan:

(a) de verzekerings- en herverzekeringsondernemingen kunnen aantonen dat het gebruik van deze gegevens passender is dan het gebruik van gegevens die uitsluitend uit een interne bron afkomstig zijn;

(b) de verzekerings- en herverzekeringsondernemingen kennen de oorsprong van de gegevens en de aannamen of methodologieën die voor de verwerking van deze gegevens worden gehanteerd;

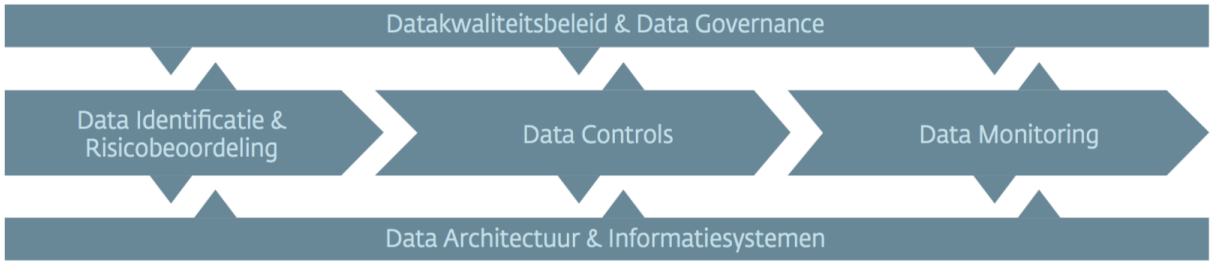
(c) de verzekerings- en herverzekeringsondernemingen onderkennen alle trends in deze gegevens en de variatie, in de tijd of naargelang van de gegevens, van de aannamen of methodologieën voor het gebruik van die gegevens;

(d) de verzekerings- en herverzekeringsondernemingen kunnen aantonen dat de onder b) en c) bedoelde aannamen en methodologieën de kenmerken van de portefeuille verzekerings- en herverzekeringsverplichtingen van de verzekerings- of herverzekeringsonderneming weerspiegelen.

Reikwijdte

Bereik van het beleid

Het datakwaliteitsbeleid strekt zich uit over de volgende vijf aandachtsgebieden die in hoofdstuk 'processen en controls' nader worden uitgewerkt:



Het datakwaliteitsbeleid heeft betrekking op de gehele AO/IC van de verzekeraar, niet alleen op de formele rapportages zoals de jaarrekening en de QRT-staten, maar met name ook op de datakwaliteit van systemen die worden gebruikt voor strategische, tactische en operationele besluitvorming.

Relevante bronsystemen

De datakwaliteit is afhankelijk van de adequaatheid, volledigheid en juistheid van de gebruikte data. De gebruikte data bevat data uit bronsystemen, maar ook data die wordt afgeleid van data uit bronsystemen, alsmede de uitkomsten van schattingsprocessen (expert judgement). De volgende systemen zijn in gebruik voor het verzamelen van de data:

[invoegen datasystemen]

Denk aan:
- Polisadministratie
- Claimsadministratie
- Financiële administratie
- Asset administratie
- Rapportagesystemen
- Actuariële tools en systemen

Aanvullende aandachtsgebieden

Onderdeel van dit beleid zijn tevens uitgangspunten voor:
- Het beheer van ICT systemen (waaronder General IT-controls);
- Uitgangspunten voor de bescherming van privacy-gevoelige informatie;
- Uitgangspunten voor het gebruik van gegevens van derden;
- Uitgangspunten voor het gebruik van end-user computing

Uitgangspunten

Uitgangspunten

Het uitgangspunt is dat de de data die worden gebruikt als input voor berekeningen, rapportages en analyses van goede kwaliteit moeten zijn en bruikbaar moeten zijn voor het doel waarvoor zij worden verzameld. Goede kwaliteit wordt hierna nader gedefinieerd.

Bij het constateren van tekortkomingen in data en/of systemen zorgt de verzekeraar voor adequate procedures voor (1) het oplossen van de geconstateerde fouten in het verleden (waaronder data cleansing) en (2) het voorkomen van fouten in de toekomst.

Voorts moet de datakwaliteit zo mogelijk meetbaar zijn. Periodiek moet worden vastgesteld dat de data plausibel is en bruikbaar is voor het doel waarvoor zij gebruikt wordt. Voor zover er modellen worden gebruikt, moeten deze voorafgaand aan het gebruik worden gevalideerd.

Als uitgangspunt geldt dat datasystemen beschikbaar en toegankelijk zijn, adequaat beveiligd, adequate back-up en dat er adequate maatregelen zijn om te voorkomen dat er ongeautoriseerde toegang plaats kan vinden of dat ongeautoriseerde mutaties worden verwerkt.

Definities

Uit artikel 82 van de Solvency II Richtlijn kan worden afgeleid dat de datakwaliteit afhankelijk is van het nauwkeurig monitoren van de volgende criteria:

- Adequaatheid: data wordt als adequaat beschouwd als zij geen materiële vergissingen, fouten of omissies bevat. De meeste hiervan worden veroorzaakt door menselijke fouten of falen van de IT-systemen.
- Volledigheid: data wordt als volledig beschouwd als zij toestaat dat de volatiliteit en onzekerheden van de trends kunnen worden gemeten en de onderliggende risico's volledig kunnen worden begrepen.
- Juistheid: data wordt als juist beschouwd als zij bruikbaar is voor het beoogde doel, en relevant voor de beoogde analyses.

Verantwoordelijkheid voor de datakwaliteit

Administratieve organisatie is het systematisch verzamelen, vastleggen en verwerken van gegevens ten behoeve van het verstrekken van informatie ten behoeve van het besturen en doen functioneren van een organisatie en ten behoeve van de verantwoording die daarover moet worden afgelegd.

Beheersing van de datakwaliteit is een essentieel onderdeel van de AO/IC en behoort daarmee tot de uiteindelijke verantwoordelijkheid van de CFO van de verzekeraar. In deze hoedanigheid is de CFO ook verantwoordelijk voor dit beleid en de vertaling daarvan binnen de organisatie.

De CFO is verantwoordelijk om ervoor te zorgen dat:
- De beheersing van de datakwaliteit (afhankelijk van de aard, omvang en complexiteit van eventuele issues) periodiek op de agenda van het bestuur staat;
- De beheersing van de datakwaliteit wordt gewaarborgd door een effectieve AO/IC;
- In samenwerking met de sleutelfuncties de kwaliteit van data wordt bewaakt, teneinde te zorgen dat de strategische, tactische en operationele besluitvorming is gebaseerd op juiste, volledige en adequate data;
- Issues in de datakwaliteit worden binnen redelijke termijnen opgelost, afhankelijk van de risico's die deze issues opleveren (waaronder het risico van non-compliance met het rapportagebeleid).

Uitgangspunten voor de ICT omgeving

Datakwaliteit is ingebed in een beheerste ICT omgeving. Een beheerste ICT-omgeving houdt in dat de general IT-controls op een volwassenheidsniveau van ten minste 3 of 4 liggen[1] (gebaseerd op het Toetsingskader Informatiebeveiliging van DNB)[2].

De interne auditfunctie stelt ten minste éénmaal per drie jaar vast dat de self assessment wordt uitgevoerd, geactualiseerd en dat de acties die hieruit volgen effectief worden opgevolgd.

Uitgangspunten voor de bescherming van privacygevoelige informatie

Voor wat betreft de opslag en het beheer van gegevens binnen de verzekeraar, waarborgt de privacy-officer[3] de adequate naleving van de Algemene Verordening Gegevensbescherming ("AVG"). De privacy-officer kan dwingende aanwijzingen geven voor wat betreft de opslag en het beheer van gegevens, teneinde te waarborgen dat de verzekeraar voldoet aan de wettelijke bepalingen.

De privacy-officer heeft een en ander nader uitgewerkt in het protocol "Bescherming privacgevoelige informatie". De compliance officer stelt jaarlijks vast dat de controls die worden beschreven, ook daadwerkelijk worden uitgevoerd en dat eventuele compliance risico's adequaat worden opgepakt.

Uitgangspunten voor het gebruik van gegevens van derden

Voor zover gegevens van derden worden gebruikt in de administratieve processen van de verzekeraar, moet hieraan een risico-analyse vooraf gaan. Op grond van deze risico-analyse wordt besloten in welke mate nadere eisen moeten worden gesteld aan het gebruik van deze informatie.

In beginsel geldt dat als informatie kritisch is voor strategische, tactische en/of operationele besluitvorming of rapportageprocessen, dat de verzekeraar kan vertrouwen op externe toetsing van de procedures die de datakwaliteit moeten waarborgen (bijvoorbeeld door een ISAE 3402 Type II verklaring).

In het geval dat deze externe bevestiging ontoereikend of niet beschikbaar is, moet de verzekeraar aanvullende controles uitvoeren om de juistheid, volledigheid en/of plausibiliteit van deze gegevens te beoordelen.

Uitgangspunten voor end-user computing

In termen van beheersing van de datakwaliteit betekent end-user computing een inherent hoger risico op fouten. Als uitgangspunt geldt dat het gebruik van end-user computing in beginsel moet worden beperkt tot die processen waarbij een hoge mate van flexibiliteit wenselijk of noodzakelijk is, zoals het analyseren en aansluiten van gegevens.

Indien er redelijke alternatieven bestaan voor het gebruik van end-user computing, dan zullen deze worden overwogen met het oog op een verbetering van de beheersing van de dataflow.

Voor zover end-user computing onvermijdelijk is in de operationele of rapportage dataflow, worden hieraan nadere eisen gesteld (zie hiervoor onder 'processen en controls').

[1] https://www.inaudit.nl/publicaties/artikelen/informatiebeveiliging-op-orde
[2] http://www.toezicht.dnb.nl/3/50-203304.jsp
[3] Ook aangeduid als "Functionaris voor de gegevensbescherming"

Data directory, data definition

Voor zover noodzakelijk worden data-elementen die deel uitmaken van de management-rapportages, de jaarrekening of de rapportage aan de toezichthouder (QRT-staten) vastgelegd en gedefinieerd.

Voor zover de aard, omvang en de complexiteit van de data dit toestaat, wordt dit als onderdeel van de accounting manual vastgelegd.

Voor wat betreft de vastlegging van de data-elementen zoals opgenomen in de QRT-staten verwijzen we naar de betreffende beschrijvingen en definities zoals vastgelegd in Uitvoeringsverordening 2015/2450, waaronder meer specifiek bijlage 1 van deze verordening (de QRT-templates) en bijlage 2 en 3 (de logfiles bij deze QRT's).

De bronnen van data zijn specifiek voor de organisatie en kunnen worden herleid aan de hand van het accounting manual.

Risicobeheersing

Inherente risico's (data)

We onderscheiden de volgende risico's met betrekking tot de datakwaliteit:

i. Inadequate data: het risico dat de gebruikte data niet accuraat is, veroorzaakt door verkeerde invoeren in de bronsystemen of het incorrect groeperen van data verderop in de dataflow, hetgeen leidt tot foutieve informatie aan het management.

ii. Onvolledige data: het risico dat de gebruikte data niet volledig is, veroorzaakt door ontbrekende gegevens in de bronsystemen of onjuiste verwerking van de data verderop in de dataflow, hetgeen tevens leidt tot foutieve informatie aan het management.

iii. Onjuiste data: het risico dat de gebruikte data niet gevrijwaard is van fouten, verkeerde interpretaties of andere tekortkomingen.

Inherente risico's (systemen)

We onderscheiden de volgende risico's met betrekking tot de datasystemen:

i. Onbevoegde toegang tot datasystemen: het risico dat onbevoegden data invoer, muteren of verwijderen;

ii. Onbekwaam gebruik van systemen: het risico dat functionarissen data invoeren, muteren of verwijderen zonder dat zij voldoende kennis hebben om de consequenties te kunnen doorzien;

iii. Verlies van toegang tot datasystemen: het risico dat systemen en/of data ontoegankelijk worden door technische of functionele fouten of uitval van systemen zonder adequate back-up;

Materialiteit & proportionaliteit

Materialiteit

Artikel 291 van de Gedelegeerde Handeling (2015/35) stelt dat: informatie als materieel aangemerkt wordt indien de weglating of onjuiste weergave ervan de besluitvorming of het oordeel van de gebruikers, inclusief de toezichthouders, zou kunnen beïnvloeden. Het criterium van de materialiteit moet worden toegepast op elke datatransactie en zal elk jaar worden getoetst.

Proportionaliteit

Van proportionaliteit is sprake als er een effectief intern control framework is opgezet om materiële fouten en ontbrekende gegevens te voorkomen. De controles om de risico's uit hoofdstuk 4 te mitigeren moeten in de juiste verhouding staan tot de schaal, aard en complexiteit van de dataprocessen.

Dit werkt twee kanten op: enerzijds rechtvaardigt het simpeler manieren van het voorkomen en opsporen van fouten en ontbrekende gegevens voor low-risk databronnen, modellen en berekeningen, maar het betekent anderzijds ook dat voor meer complexe databronnen, modellen en berekeningen meer verfijnde methoden noodzakelijk zijn.

Voor de wijze van toepassing van materialiteit en proportionaliteit en de nadere definitie verwijzen we naar het rapportagebeleid.

Risicobereidheid

Voor de risicobereidheid met betrekking tot datakwaliteit verwijzen we naar het rapportagebeleid.

Het uitgangspunt is dat data geen fouten mogen bevatten waarvan de omvang kan leiden tot materiële verschillen in de management-rapportages, de berekening van de solvabiliteit en/of de statutaire jaarrekening.

Interne control framework

Het interne control framework is ontworpen om de risico's van de dataflow te beheersen en de vereiste datakwaliteit te waarborgen.

Het zorgt voor een overzicht van wettelijke vereisten, zakelijke vereisten, daarmee samenhangende risico's en interne controles om deze risico's te beheersen. Het zal regelmatig worden getoetst op effectiviteit.

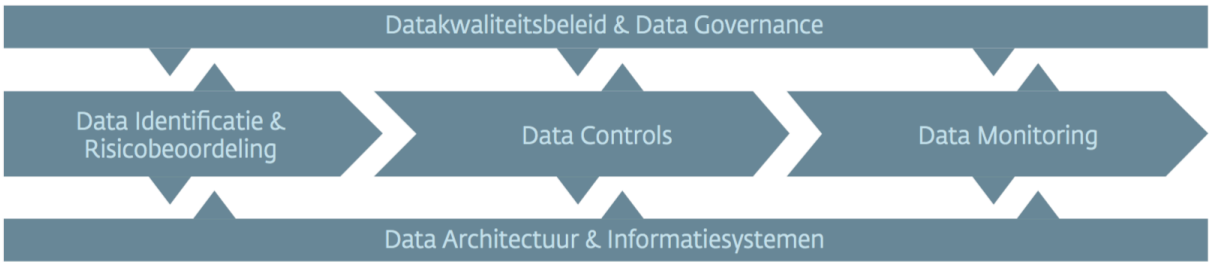
De belangrijkste beheersmaatregelen zijn:

- Adequate vastlegging van processen, procedures en instructies
    - Adequate toepassing van business rules, validaties en geautomatiseerde controles,
    - Adequate functiescheidingen
    - Adequate data governance
    - Toetsing door de interne (IT) auditor op de naleving van het beleid en de controls, waaronder de ITG controls

- Periodieke analyse van de data
    - Interne controle op de datakwaliteit (financiële functie)
    - Toetsing van de datakwaliteit door de actuariële functie
    - Toetsing van de betrouwbaarheid door de externe accountant

Processen en controles

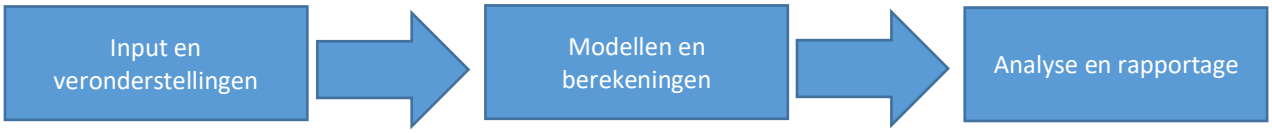
In lijn met het Guidance document van DNB is dit hoofdstuk als volgt nader uitgewerkt:



Voor wat betreft de data governance verwijzen we naar het hoofdstuk “Governance” en voor wat betreft data architectuur & informatiesystemen verwijzen we naar het ICT-beleid.

Data identificatie & risicobeoordeling

Onderstaand zijn op hoofdlijnen de belangrijkste datasystemen weergegeven:



VTA Polis	Rapportagesysteem	Rapportage
VTA claims	Actuariële toetsing	
Financiële administratie		
Assets		
Actuariële toetsing		

Uitgangspunt

Een goede beheersing van de datakwaliteit in de hele keten van vastleggen tot en met rapporteren, begint met een goede adequate vastlegging van transacties en mutaties. Fouten in de vastlegging en correcties daarop maken het inzicht diffuus en kunnen leiden tot nieuwe fouten. Daarom geldt als uitgangspunt:
“Zorg (in één keer) voor een juiste en volledige vastlegging in de bron”

Verantwoordelijkheid

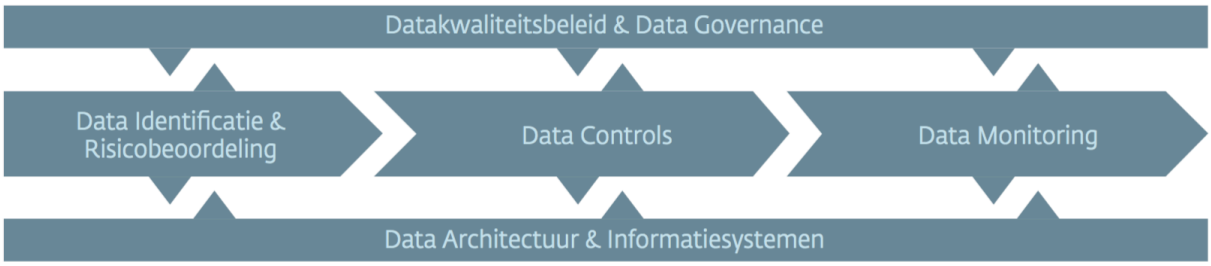
Voor elk datasysteem is een manager verantwoordelijk. De verantwoordelijke manager moet zorgen dat de data in het datasysteem adequaat, juist en volledig zijn. Bij overdracht van data is de verstrekker van de data verantwoordelijk voor de juistheid, volledigheid van de data die aan de interface worden doorgegeven.

Identificatie

De manager die verantwoordelijk is voor het datasysteem beoordeelt welke data-elementen kritisch zijn (“KDE” - kritische data elementen) en beoordeelt welke risico’s de juistheid en de volledigheid van deze data bedreigen. Hiervoor worden analyses uitgevoerd. Zo nodig wordt ook de flow van data door systemen hierbij betrokken, alsmede de algoritmes die worden gebruikt om data te verrijken of te comprimeren.
Deze beoordeling wordt afgestemd met de risicomanager.

Risico-analyse

Periodiek stelt de risico manager vast dat de controls die managers hebben ingericht om de kwaliteit van de data in de datasystemen te bewaken adequaat zijn. De risicomanager stelt hiertoe een risico-analyse op en bewaakt de daadwerkelijke uitvoering van de gedefinieerde beheersmaatregelen (controls).



Data controls & Monitoring

Het management zorgt voor adequate waarborgen voor het bewaken van de kwaliteit van de data. Deze maatregelen omvatten zowel preventieve maatregelen als repressieve controles.

Dataverwerking met behulp van end-user computing en het gebruik van expert judgement betekenen een inherente verhoging van het interne controlerisico. Deze bronnen van (verrijkte) data hebben een impliciet hoger risico op beïnvloeding en/of fouten. Het gebruik hiervan moet zo mogelijk worden beperkt.

Voor het gebruik van end-user computing hebben we in dit hoofdstuk specifieke uitgangspunten gedefinieerd.

De effectiviteit van de maatregelen van beheersing wordt periodiek vastgesteld. Het management ("eerste lijn") is verantwoordelijk voor goede data. De governance-functies ("2e/3e lijn") borgen de monitoring.

Preventieve bewaking datakwaliteit

Onderdeel van de verantwoordelijkheid voor de data in het datasysteem betekent ook dat de betreffende manager maatregelen treft om de kwaliteit van de data vast te stellen. Hiervoor kan de manager gebruik maken van:

- Analyse van mogelijke risico's en maatregelen
- Geprogrammeerde controles
- Beoordeling van de uitval
- Signaallijsten
- Aansluitingen en verbandscontroles

Bewaking datakwaliteit achteraf

Het is onvoldoende om alleen maar te vertrouwen op de controles vooraf. Het is ook van belang dat achteraf wordt vastgesteld dat de hypothese vooraf dat de preventieve maatregelen effectief waarborgen dat geen fouten kunnen optreden, achteraf worden vastgesteld (in elk geval voor data-elementen die kritisch zijn). Indien systemen slechts beperkt voorzien in preventieve maatregelen, moeten repressieve maatregelen worden uitgebreid.

Voor het achteraf vaststellen van de effectiviteit van de preventieve maatregelen, kan de manager gebruik maken van:

- Rapportages en cijferanalyses;
- Beoordeling plausibiliteit
- Aansluiting tussen systemen en andere verbandscontroles
- Aflettering van controlerende tussenrekeningen
- Detailcontroles, steekproeven en eigen waarneming
- Data-analyse tooling

Data-incidenten

Het vastleggen en signaleren van fouten in rapportages of fouten in de bronsystemen heeft als doel om oorzaken te analyseren en hierop adequate maatregelen te treffen.

Data incidenten worden gemeld en vastgelegd door de risicomanager en door de risicomanager besproken met de verantwoordelijke manager en de CFO. De CFO bepaalt op welke wijze deze issues worden opgepakt (welke prioriteit, wie en wanneer gereed).

Het preventief voorkomen van fouten is efficiënter dan het achteraf corrigeren.
Het uitgangspunt moet zijn dat alle transacties en mutaties in één maal juist en volledig worden vastgelegd.

Betrokkenheid van risicomanagement

De risicomanager stelt vast dat de vastgelegde beheersmaatregelen (zowel preventief als repressief) gezamenlijk effectief zijn om vast te stellen dat de data in de systemen leiden tot een beheerste bedrijfsvoering. De risicomanager houdt tevens het register bij met data-incidenten (“actielijst datakwaliteit”).

De risicomanager houdt een risicoregister bij met beheersmaatregelen en stelt vast dat beheersmaatregelen daadwerkelijk worden uitgevoerd.

Betrokkenheid van de actuariële functie

De actuariële functie heeft op grond van haar charter een verantwoordelijkheid om de geschiktheid van de data te beoordelen. Indien en voor zover de actuariële functie vaststelt dat de data beperkingen qua kwaliteit kennen, worden deze als data incidenten gemeld bij de risicomanager.

Binnen haar deskundigheid voert de actuariële functie controles uit om invulling te geven aan haar verantwoordelijkheid.

Betrokkenheid van de interne auditfunctie

De interne auditfunctie voert op grond van haar risico-analyse en jaarplan audits uit, waarbij zij zelfstandig en onafhankelijk tot een oordeel komt omtrent de effectiviteit van de beheersmaatregelen. Indien zij hierbij constateert dat brondata, interfaces, rapportages en/of analyses fouten of beperkingen bevat, worden deze als data incidenten gemeld bij de risicomanager.

Binnen haar deskundigheid voert de interne auditfunctie controles uit om invulling te geven aan haar verantwoordelijkheid.

Beheer van end-user computing (EUC-controls)

Het gebruik van end-user computing is soms technisch onvermijdelijk en in sommige gevallen efficiënter dan het inrichten van datawarehouses of andere technische oplossingen. Bij end-user computing denken we aan Excel en/of Access toepassingen voor andere doeleinden dan het ad-hoc uitvoeren van een analyse of een controleberekening.

Het gebruik van EUC is om een aantal redenen inherent minder beheersbaar en om deze reden moeten de volgende stappen worden doorlopen bij het gebruik van EUC:

1. Bepaal of een EUC toepassing een kritische EUC toepassing is.

Bij een kritische EUC’s kunnen fouten leiden tot materiële fouten in de management rapportages, de QRT-staten en/of de jaarrekening. EUC-toepassingen die in operationele processen routinematig worden gebruikt vallen eveneens onder kritische EUC-toepassingen.

2. Kritische EUC-toepassingen worden beheerd

Voor elke kritische EUC-toepassing is een eigenaar benoemd en een plaatsvervangend eigenaar. De eigenaar is verantwoordelijk voor het versiebeheer en het up-to-date houden van het tool. De eigenaar zorgt voor adequate beveiliging van het tool (zowel de blanco-versies als de toegepaste versies).

3. Ontwerp van de EUC-toepassing

In het ontwerp van kritische EUC-toepassingen worden invoer, bewerking en uitvoer zoveel mogelijk gescheiden. Bewerkingen en uitvoervelden worden zoveel mogelijk beschermd, met dien verstande dat het beheer van wachtwoorden niet mag leiden tot een key man risk.

De EUC toepassing omvat voor zover mogelijk controletotalen en verbandscontroles aan de hand waarvan de goede werking van het tool kan worden vastgesteld, respectievelijk op grond waarvan verschillen en/of uitval kunnen worden geconstateerd.

De EUC toepassing heeft een gebruiksaanwijzing en is voor hergebruik ontworpen. Indien noodzakelijk is het ontwerp gedocumenteerd en wordt training verzorgd (en beschikbaar gehouden) over het gebruik van het EUC tool.

4. Validatie van en Change management op de EUC-toepassing

Kritische EUC toepassingen worden door een van de ontwerper onafhankelijke medewerker getoetst op effectieve werking en het vermijden van harde waarden en andere mogelijke bronnen van fouten. Hierbij worden deze toepassingen getoetst met theoretische data om de individuele stappen op juistheid en volledigheid te toetsen, alsmede met echte productiedata. Zo mogelijk wordt het tool gecontroleerd met onafhankelijke ad-hoc berekeningen.

Nieuwe versies van het tool worden eerst gebouwd en ontworpen, dan getoetst en pas na akkoord in productie genomen. De eigenaar van het tool zorgt hij te allen tijde een ‘schone’ kopie van de laatste versie beschikbaar heeft.

5. Opslag van tools en data, inclusief versiebeheer

Om een effectieve audit-trail te waarborgen wordt bij het gebruik van kritische EUC-tools elke versie die tot een rapportage leidt opgeslagen (gebruikte basisdata plus het tool waarin deze data zijn bewerkt). Voorkomen wordt dat deze tool nadien onbedoeld wordt gewijzigd of dat data per abuis worden overschreven. Oude versies van het tool worden beschikbaar gehouden in lijn met de regels voor bewaring van data.

Governance

Het “three-lines-of defense”-model voorziet in drie niveaus van functies die betrokken zijn bij effectief risicomanagement:

1. Functies die risico’s beheren en beheersen
2. Functies die risico’s overzien
3. Functies die voorzien in onafhankelijk oordeel

CFRO als eindverantwoordelijke

In de eerste lijn vallen de operationele medewerkers en de eventuele uitbestede actuariële werkzaamheden. De CFRO is eindverantwoordelijk voor het beheren en beheersen van de risico’s, alsmede voor het implementeren van de juiste maatregelen om het proces te verbeteren. Tevens is de CFRO verantwoordelijk voor het uitvoeren van de dagelijkse risico- en controleprocedures.

Data governance

Data governance kan als een separaat onderdeel worden gezien van de governance organisatie. Binnen InRisk Schadeverzekeringen NV, beschouwen we data governance als een impliciet onderdeel van de administratieve organisatie.

De verantwoordelijkheid voor data, risico-analyses en controls ligt bij de managers die voor de processen en ondersteunende systemen verantwoordelijk zijn. Binnen InRisk Schadeverzekeringen NV bestaat geen noodzaak om aanvullend een data-directory op te stellen, data-elementen te definiëren en toe te wijzen aan eigenaren en data stewards.

Rol van de sleutelfuncties

De tweede lijn zorgt ervoor dat risico’s goed gemanaged worden binnen de risicobereidheid. Tevens zorgen zij ervoor dat de processen en procedures die in dit en onderliggende documenten worden beschreven juist worden uitgevoerd.

De actuariële functie heeft een specifieke rol, zoals beschreven is in Artikel 48, 1c van de Solvency II Richtlijn. Deze functionaris beoordeelt of genoeg gegevens worden gebruikt bij de berekening van technische voorzieningen, en zij beoordeelt de kwaliteit ervan.

De derde lijn wordt ingevuld door de interne auditor. Zij voorzien de directie en het hogere management van uitvoerige, onafhankelijke en objectieve rapportage over het functioneren van de organisatie.

Externe controle

Tenslotte betrekt de externe accountant in zijn oordeel omtrent de getrouwheid van de jaarrekening zijn bevindingen met betrekking tot de datakwaliteit en het beheersingsproces.

Vaststellen en goedkeuren beleid

Dit beleid is opgesteld en goedgekeurd door het bestuur.

Het rapportagebeleid wordt jaarlijks geëvalueerd en indien nodig bijgesteld.
Voor wijzigingen van het datakwaliteit beleid is voorafgaande goedkeuring van het bestuur vereist.

Het rapportagebeleid en eventuele wijzigingen daarvan worden, voorafgaand aan definitieve vaststelling door het bestuur, ter informatie en bespreking verstrekt aan de audit commissie, als vertegenwoordigend orgaan van de raad van commissarissen.

Wijzigingen worden bijgehouden op het voorblad versiebeheer.

Goedkeuring door het bestuur,
namens deze,