SPRENKELS & VERSCHUREN
ACTUARISSEN CONSULTANTS

RiskTransparant

IT Risicobereidheid
"…het IT dossier is een must geworden voor elke bestuurder…"

In deze eerste serie uit een reeks van zeven delen, delen wij graag onze kennis met u over risicomanagement. Dit keer staat het dossier IT Risicomanagement centraal.

Aanleiding

DNB heeft het thema Informatie Technologie (IT) goed in het vizier. Hiermee komt er een normatieve werking naar de pensioenfondsen én haar dienstverleners. Dit zal effect hebben in de hele keten van (administratieve) dienstverlening. Van internetcontent partijen tot en met actuariële bureaus, groot en klein. De verhoogde attentie is mede te danken aan de nieuwe privacywetgeving (per 1 januari 2016) én aan het feit dat de impact van de geautomatiseerde systemen steeds groter wordt. Tel hierbij op de verscheidenheid aan partijen die aan tafel zitten bij het Bestuur voor de totale dienstverlening voor pensioenfondsen, ieder met z'n eigen (IT)systeem, beleid en visie.

Wie garandeert de juistheid, tijdigheid, volledigheid en verwerking van data die van het ene naar het andere systeem gaan? Het fonds blijft, ongeacht de afspraken met derden in uitvoeringsovereenkomsten en SLA's, te allen tijde eindverantwoordelijk voor de data. Volgens DNB is artikel 3:17 WfT en ter uitvoering hiervan artikel 20 lid 1 van het Besluit prudentiële regels (Bpr; betreffende de waarborging van voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens) voor pensioenfondsen bovendien van overeenkomstige toepassing. Verder is er al van oudsher een categorie IT Risico opgenomen in de FIRM analyse van DNB. Dit onderdeel is in risicoassessments vaak onderbelicht geweest en staat nu in de schijnwerpers. Het dossier: IT in de keten, is een must geworden voor elke bestuurder.

Nu zijn er twee vragen, die vaak gesteld worden: *wat te doen én hoe te doen*. Deze twee vragen staan centraal in dit artikel.

Wat te doen?

Een focus op IT aan de bestuurstafel en binnen het VO, als ook de RvT is essentieel, gezien de afhankelijkheid van IT voor een beheerste en integere bedrijfsvoering. Nog los van het compliance perspectief als hierboven beschreven. Door regelmatig stil te staan bij de volgende 5 vragen, kunt u inzicht en bewustwording verkrijgen c.q. vergroten:

- Zijn er of zien we aankomende veranderingen in onze doelstellingen die een impact hebben op of door IT en/of privacy? Zo ja, welke processen zijn dit en welke systemen worden hierdoor geraakt?
- Zijn er of zien we aankomende veranderingen bij onze uitvoerders die een impact hebben op of door IT en/of privacy? Zo ja, welke processen zijn dit en welke systemen worden hierdoor geraakt?
- Zijn er incidenten te herleiden naar IT en/of privacy? En worden alle incidenten ook gemeld aan het bestuur?
- Het voeren van de dialoog aan tafel van het bestuur en in de administratieve keten: wat is de dialoog hierover met uw uitvoerders in de keten, silo en integraal?
- Het monitoren en rapporteren over het IT beleid intern (binnen het fonds) en vanuit uw uitvoerders (buiten het fonds).

De dialoog aan de bestuurstafel zou daarom ook moeten gaan over IT en andere niet financiële risico's. Wij zien in de praktijk dat het onderwerp 'beleggingen' prominent op de bestuurstafel aanwezig is. Uiteraard is dit een zeer essentieel onderdeel, maar zijn de niet financiële risico's hierdoor niet minder relevant.
Wat verder te doen? Het hebben van een eigen visie op IT en informatiebeveiliging. In onze visie zouden de volgende zaken meegenomen kunnen worden (niet limitatief en niet chronologisch) in uw IT beleid.

Onderdeel IT Beleid	Doel van dit onderdeel	Korte toelichting
Scope en doelgroep	Document is bestemd voor en is geldig tot en met.	*Voor wie, waarvoor en welke periode.*
IT Risk Appetite	Vertrekpunt voor uw IT Beleid door het definiëren van uw principes. Wat wenst u niet te hebben als het om IT gaat?	*Uw IT risicobereidheid.*
IT beleid en Informatieplanning	Het geformuleerde en geaccordeerde beleid door het voltallig bestuur.	*Uw uitgangspunten voor IT, bijvoorbeeld u wenst alleen gebruik te maken van Microsoft producten en u werkt alleen met de voorlaatste versie van een applicatie, wat zijn de kosten van IT?*
IT Risicobewustzijn	Uw intrinsieke motivatie om ook voor IT in control te zijn en het gesprek te hebben aan de bestuurstafel. Incluis de Permanente Educatie voor dit onderwerp.	*Hoe houdt u het onderwerp onder de aandacht bij het Bestuur en uw uitvoerders in de gehele keten.*
IT organisatie inrichting en IT kennisontwikkeling en borging	Wat zijn de verantwoordelijkheden voor IT binnen het fonds en bij uw uitvoerders? Op welke wijze wordt er aandacht besteed aan kennis- ontwikkeling en kennisborging? Ook van applicaties die verouderd zijn.	*Uw IT governance en IT HR & Kennis. Is er sprake van IT counter vailing power?*
IT Data- & Assetmanagement	Hoe ziet uw applicatie landschap eruit van hardware en software? Wie gebruikt welke applicatie en heeft welke rechten? Wat is de data governance? Wat is de IT Complexiteit?	*Welke applicaties: (open source) hardware en software zijn er en wie zijn de gebruikers, welke dataclassificatie wenst u? Is er sprake van exclusiviteit ,integriteit, continuïteit, controleerbaarheid, authenticiteit en onweerlegbaarheid.*
IT Risk & Compliance	Wat is het IT Risk & Compliance denkmodel? Hoe sluit dit aan bij uw reguliere model (indien u met een andere methodologie werkt voor IT). Wat is uw DNB volwassenheid voor IT?	*Uw IT risk & IT compliance, ook voor de licenties die u gebruikt. Het houden van een (IT) Keten risicoanalyse en voor cloud applicaties.*
IT Controls	Hoe gaat u controle houden op het IT proces? En waar in het proces gaat u controls implementeren? Hoe voorkomt u stapelen van controls?	*Leverancierscontrole, controls in het proces, cryptografie, communicatie (secured line met DNB en het uitnodigen van IT managers van uitvoerders één keer per jaar).*
IT Proces- & Cost Management	Heeft u begrip voor reguliere en wijzigende IT processen? En hoeveel budget heeft uw IT organisatie?	*Procesoptimalisatie en maximalisatie onder huidige omstandigheden en wijzigingen, run & change.*
Business Impact Analyse	Welke processen zijn essentieel en in welke mate en hoe is de back-up en/of recovery ingeregeld?	*Welke processen zijn essentieel en wat is het effect bij uitval.*

Nu de *wat* vraag is besproken, maken we een doorkijk naar de *hoe* vraag.

Hoe te doen?

De eerste stap is om uw IT risicobereidheid vast te stellen, door de volgende twee vragen te stellen:
1: Wat is uw risicobereidheid?
2: Wat wenst u niet dat er gebeurt? Dit zijn uw leidende principes.

Om dit proces gestructureerd te laten verlopen kunt u het *best practice* RAVC© model hanteren. Dit geeft u houvast in het proces, geeft duidelijk structuur en verhoogt het risicobewustzijn op dit onderdeel.

De tweede stap is om uw leidende principes te verwoorden en op te nemen in uw eigen IT-beleid, waar informatiebeveiliging en privacy onderdeel van uit maken. Zo bent u niet weer aan het stapelen en kunt u uw risicobereidheid integreren in uw beleid.

De derde stap is om uw beleid concreet te vertalen naar meetindicatoren en deze op te nemen in uw contracten of SLA's. U bent zo leidend en niet volgend in het IT debat.

De vierde stap is om het IT dossier onderdeel uit te laten maken van uw ISAE 3402 scope. Nu zien we vaak dat dit niet het geval is. Door het proces zo te doorlopen kunt u ook een grotere meerwaarde creëren met uw ISAE-rapportage en is het niet alleen een dik pak papier, waarvan u zou kunnen denken: 'de accountant heeft er al naar gekeken'.

De vijfde stap is om de bovenstaande vier punten te borgen, monitoren en te rapporteren.

Kortom: in 5 concrete stappen naar een hoger vertrouwen in uw fonds!

Meer informatie óf meer kennis delen? Download de andere artikelen op www.sprenkelsenverschuren.nl of neem contact op met uw vaste contactpersoon bij Sprenkels & Verschuren.