Amsterdam – 13 juli 2020

Probability snapshot

Verbeteren van IT-volwassenheid, en het DNB IT-raamwerk

Beste lezer,

De kwaliteit van de beheersing van IT en informatiebeveiliging is van groot belang voor pensioenfondsen en zal ook alleen maar blijven toenemen. DNB heeft dat ook al jaren in het vizier en zet daar steeds meer op in bij de toezichtagenda. Het raamwerk dat DNB hanteert en de kritische rapporten die soms uit de onderzoeken komen leiden tot onzekerheid bij pensioenfondsen. In deze snapshot geven we meer inzicht in hoe u om kunt gaan met IT, informatiebeveiliging en het IT-raamwerk dat DNB hanteert. Hierin beschrijven we dat ook als er nog flinke stappen gemaakt moeten worden, u zelf de touwtjes in de hand kunt houden en er echt geen al te dure trajecten aan verbonden hoeven te zitten.

Heeft u hierover vragen of zou u dieper over dit onderwerp in gesprek willen gaan, dan nodigen wij u van harte uit om contact op te nemen met een van onze ICT & Security consultants voor een vrijblijvend gesprek.

Met vriendelijke groet,

Team Risk Management

Probability & Partners

Inleiding

DNB heeft dit jaar voor de tweede keer de informatiebeveiligingsmonitor[i] uitgebracht waarin een aantal waarnemingen worden gedeeld die van belang zijn voor financiële instellingen. Daarnaast voert DNB al enige jaren diepgaande IT-onderzoeken uit bij onder andere pensioenfondsen[ii]. Dat is ook belangrijk, gezien de impact die IT heeft en de afhankelijkheid die pensioenfondsen hebben.

DNB heeft hiervoor een raamwerk opgesteld dat gebaseerd is op CobIT, een auditstandaard voor het beoordelen van IT-omgevingen. Dit is echter een zeer uitvoerige standaard, omdat alle aspecten van IT daarin geraakt moeten worden en de standaard ook voor de meest complexe organisaties toepasbaar moet zijn. En daar raak je direct de uitdaging voor pensioenfondsen. DNB heeft CobIT behoorlijk uitvoerig doorgevoerd in het raamwerk voor pensioenfondsen, terwijl pensioenfondsen doorgaans zeer beperkt zijn in omvang en complexiteit. Een diepgaand onderzoek door DNB op basis van een vergaand auditraamwerk is een recept voor een rapport vol bevindingen. En dat zien we dan ook vaak gebeuren.

Enerzijds vanwege de zeer uitvoerige aanpak van DNB die daar een speerpunt van heeft gemaakt. Anderzijds omdat de volwassenheid van IT-management en IT-risk management bij veel pensioenfondsen zeker nog stappen moet maken.

Nuttige oplossing?

En dan moet er actie ondernomen worden om met de bevindingen van DNB aan de slag te gaan. Of in aanloop naar een aankomend onderzoek door DNB wil een pensioenfonds de zaken zo goed mogelijk op orde hebben om zo'n kritisch rapport te kunnen voorkomen. In veel gevallen worden er IT-experts ingehuurd om in kaart te brengen waar de gaten zitten (als er nog geen DNB-onderzoek is geweest) en om deze op te lossen. Daarbij worden kosten nog moeite gespaard. Er volgen langdurige en kostbare trajecten om een DNB-proof IT-raamwerk in te regelen geheel conform de CobIT-standaarden.

Levert dat wel de juiste oplossing voor het fonds? Het fonds wil zeker weten dat DNB het goed zal vinden. De angst voor de uitkomsten van het DNB IT-onderzoek drijft fondsen tot, in onze ogen, te uitvoerige raamwerken. En deels zal dit in gevallen ook gedreven zijn door onvoldoende bekendheid met IT en de eigen IT-omgeving, waardoor 'blindgevaren' wordt op het advies van IT-experts.

In de meeste gevallen zal het uiteindelijk ingerichte raamwerk niet de gewenste oplossing zijn voor het pensioenfonds. Het is omslachtig en theoretisch, vaak veel doublures met andere beleidsstukken die het fonds al heeft en draagt niet direct bij aan de dagelijkse gang van zaken. Het overgrote deel van het beleid zal nooit gelezen of toegepast worden. Hoeveel, en hoe diepgaand beleid heb je als pensioenfonds nodig over encryptiestandaarden en het beheer van encryptiesleutels, of over verschillende netwerktypologieën die mogelijk zijn? Je kunt er een boekwerk over schrijven, maar het is doorgaans weinig relevant voor een pensioenfonds.

Het juiste accent

Is het IT-raamwerk van DNB dan allemaal onzin? Uiteraard niet. Er zitten veel zeer nuttige onderwerpen in. Je moet bijvoorbeeld goed weten welke gegevens je hebt en hoe je daarmee om wilt gaan. Je wil duidelijk hebben wie waarvoor verantwoordelijk is. Je moet gedegen afspraken hebben met je uitbestedingspartijen, bijvoorbeeld over de wijze waarop ze met jouw gegevens omgaan en hoe je samen wijzigingen in de IT aanpakt.

Maar houdt in gedachten dat CobIT een generiek raamwerk is dat ook bedoeld is om complexe techbedrijven zoals Google, Cisco of Microsoft in te vangen. En een raamwerk dat goed is voor dat soort bedrijven zal doorgaans niet een op een op een 'eenvoudig' pensioenfonds passen.

Het is daarom van belang om het accent op de juiste plek te leggen. Weeg goed af welk deel van toepassing is op het pensioenfonds en welk deel niet. Of minder van toepassing. Bepaal de diepgang die voor jouw

pensioenfonds van belang is en stel de juiste prioriteiten. Veel pensioenfondsen hebben nog best een stap te maken in de volwassenheid van de IT-omgeving. Zeker wanneer het aankomt op informatiebeveiliging. Maar alles in een keer perfect proberen te maken is wellicht niet realistisch of gewenst. Als de stap groot is die nog gemaakt moet worden, dan kan het goed zijn om de aanpak in fasen te verdelen: eerst naar beter (goed genoeg), daarna naar uiteindelijk gewenst.

Niet voor DNB, maar voor jezelf

Onthoud dat het verbeteren van de beheersing rondom IT en informatiebeveiliging iets is dat je voor jezelf doet. Voor je eigen pensioenfonds en voor de eigen deelnemers. Je doet dat niet voor DNB. Bepaal daarom waar je voor jezelf de lat wilt leggen. En het raamwerk van DNB kan daarbij een handige tool zijn om de onderwerpen de revue te laten passeren. Bepaal vervolgens zelf in welke mate ieder onderwerp van toepassing is op jouw pensioenfonds en hoe diepgaand het onderwerp uitgewerkt moet worden. Zodra dat van alle onderwerpen is gedaan, kun je bepalen in hoeverre dat een behapbaar geheel is of dat er prioriteiten gesteld moeten worden.

Als je op deze manier vaststelt wat het einddoel is en wat de route is om daar te komen, dan heb je ook direct een goed verhaal naar DNB. De toezichthouder is er immers ook niet op uit om kritische rapporten te schrijven. Hij wil dat er voldoende aandacht is voor IT en informatiebeveiliging, dat het pensioenfonds dat serieus aanpakt en uiteindelijk – binnen niet al te lange termijn – een goed beheerste omgeving heeft. Je hoeft niet het raamwerk van DNB tot in ieder detail uitgewerkt en geïmplementeerd te hebben. Maar je moet wel uit kunnen leggen waarom je doet wat je doet.

Wat je gaat (of laat) maken moet vooral werkbaar zijn voor het eigen pensioenfonds, voor de eigen organisatie. Je hebt niets aan een beleid dat zo uitgebreid en theoretisch is dat niemand meer snapt wat er nou eigenlijk echt moet gebeuren. Zo'n beleid belandt in de kast. Daar wordt de beheersing niet sterker van. Je kunt het beleid beter beknopt en to the point houden en begrijpelijk. Vervolgens is het van belang – voor jezelf, maar ook voor bijvoorbeeld de toezichthouder – dat het beleid en de uitvoering daarvan aantoonbaar zijn. Je moet kunnen laten zien dat je doet wat er in het beleid is beschreven en je moet kunnen laten zien dat dat ook werkelijk effect heeft. Ook voor jezelf, om te kunnen evalueren hoe het beleid werkt en of er wellicht nog verbeterslagen gemaakt moeten worden.

Conclusie

Het DNB IT-raamwerk is erg uitgebreid, generiek en veelal niet op alle onderwerpen met evenveel diepgang van toepassing op een 'eenvoudig' pensioenfonds. Maar het raakt wel de belangrijke punten en is een handige tool om te beoordelen welke stappen u nog wilt nemen.

1. Bepaal per onderwerp de **relevantie** voor uw pensioenfonds en de diepgang waarmee het uitgewerkt moet worden.
2. Voer een **gapanalyse** uit van de werkelijkheid ten opzichte van de uitkomst van stap 1. Dus niet ten opzichte van het gehele DNB IT-raamwerk, want dan vergelijkt u uw IT met die van organisaties als Google.
3. Bepaal of het oplossen van de gaps in een keer **behapbaar** is of niet.
4. Zo niet, stel dan **prioriteiten** vast voor de onderwerpen/gaps en breng eventueel **fasen** aan om in stappen naar het gewenste volwassenheidsniveau te komen.

Wat kunnen wij voor u betekenen?

Met betrekking tot de inrichting van de IT-beheersing kunnen wij op verschillende manier helpen:

- Helpen met uw SOLL-situatie in kaart te brengen: welke onderwerpen van het raamwerk zijn voor u relevant en op welk volwassenheidsniveau wilt u daarbij komen?
- We kunnen u helpen met het maken van de gapanalyse om vast te stellen welke stappen nog genomen moeten worden om aan uw gewenste SOLL-situatie te voldoen.
- Maken van een verbeterplan om van IST naar SOLL te komen.
- Opstellen en implementeren van beleid en beheersing.

En als u al een partij in de hand heeft voor een dergelijk traject, dan kunnen wij bijvoorbeeld:

- Second opinion: is het wel nodig om zo veel geld uit te geven, of om zo'n lang traject in te gaan?
- Quality assurance op verbetertraject: als het een omvangrijk traject is (qua tijd en geld) en u wellicht niet zelf alle expertise in huis hebt om het project (kwalitatief) te monitoren, kunnen wij op gezette tijden met u meekijken of het project nog wel zal gaan leveren wat de bedoeling is.
- Audit op resultaat: na afloop wilt u immers zekerheid hebben dat de nieuwe werkelijkheid ook werkelijk voldoet aan de vooraf door u gestelde SOLL-situatie. Daar kunnen wij voor u een audit op uitvoeren.

Contact

Jeroen Kinders Vroklage

Risk management consultant
jeroen.kindersvroklage@probability.nl
06 - 51 55 66 53

Renze Munnik

Risk management consultant
renze.munnik@probability.nl
06 - 19 28 06 28

Pim Poppe

Managing partner
pim.poppe@probability.nl
06 - 19 88 34 71

[i] DNB informatiebeveiligingsmonitor: https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-pensioenen/nieuwsbrief-pensioenen-mei-2020/index.jsp

[ii] Bijvoorbeeld: https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-pensioenen/NieuwsbriefPensioenenfebruari2018/index.jsp, https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-pensioenen/nieuwsbrief-pensioenen-april-2019/dnb383568.jsp