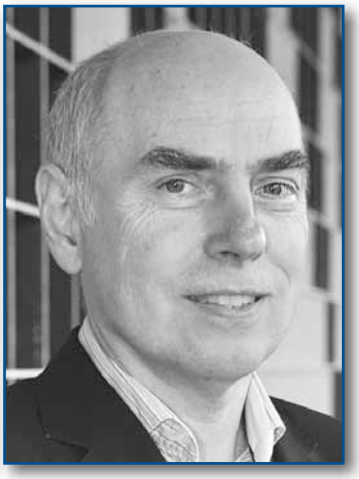
IT in control aan de bestuurstafel

Pensioenfondsen hebben hun kernactiviteiten vaak vrijwel volledig uitbesteed aan daartoe gespecialiseerde dienstverleners. Daarbij is een trend waarneembaar van verdergaande oprekking van de uitbestedingsketens, technologische innovatie en legacyproblemen, in combinatie met een veranderend pensioenstelsel. De toename van het gebruik van cloudoplossingen leidt tot een veranderd risicolandschap en toezicht. Het zorgt voor een steeds grotere vraag naar zekerheid en transparantie over de beheersing van de risico's die met de inzet en ontwikkeling van IT gepaard gaan, terwijl de IT-functie letterlijk en figuurlijk steeds verder van de bestuurstafel af komt te staan. Weet het fonds welke partijen betrokken zijn bij het proces en zijn de risico's voldoende bekend? En hoe blijft de fondsbestuurder in control over de IT-risico's?

De wettelijke eis voor integere en beheerste bedrijfsvoering verplicht de bestuurder om verantwoordelijkheid te nemen voor de beheersing van de risico's die het pensioenfonds loopt. De inrichting en uitvoering van de primaire bedrijfsvoering – vermogensbeheer en pensioenadministratie – is simpelweg niet mogelijk zonder een betrouwbare en efficiënte ondersteuning door IT-systemen.[1] Fondsbestuurders ervaren het als lastig om verantwoordelijkheid te nemen voor de inrichting en het functioneren van de IT-functie van het fonds. Dat komt vooral doordat de kernactiviteiten vaak vrijwel volledig zijn uitbesteed aan daartoe gespecialiseerde dienstverleners. Bij deze uitbesteding is een duidelijke trend waarneembaar van een toenemende complexiteit van de IT-ketens. De lengte van de ketens neemt toe door onderuitbesteding: meer schakels van gegevensverwerking en -opslag om te beheersen.

Tegelijkertijd is sprake van veranderingen op het gebied van de beheersbaarheid van IT-oplossingen die in de uitbestedingsketens worden toegepast doordat nieuwe technologieën worden gebruikt of oude technologieën in stand worden gehouden. Dit alles in een samenleving die steeds meer wordt gedreven door digitalisering en technologie en wordt gekenmerkt door cyberrisico's. Data moet in een steeds hoger tempo beschikbaar zijn en worden uitgewisseld en uitvoerders zetten nieuwe technologieën in, zoals robotica, platformstrategieën, kunstmatige intelligentie, big data en algoritmen. Deze ontwikkelingen doen zich met name voor op het niveau van de uitvoerder en diens omgeving. De pensioenfondsbestuurder is hier niet direct bij aangehaakt, waardoor de IT-functie steeds verder van de bestuurder en de bestuurstafel af komt te staan.

De IT-functie komt steeds verder van de bestuurder en de bestuurstafel af te staan



Dennis Stabel en Marcel Baveco
D. Stabel MSc RE is managing partner en drs. ir. M.P.P. Baveco RE is director, beiden bij KoutersVanderMeer, bureau voor prestatieverbetering op het gebied van IT-beheersing en technologische innovatie

KLOOF

De hiervoor beschreven ontwikkelingen kunnen leiden tot een kloof tussen de verwachtingen van het fonds en de IT-strategie van de uitvoeringspartner. Zo kan een uitvoeringspartner belang hebben bij het neerzetten van een stabiele informatievoorziening en bijbehorend IT-landschap, terwijl het fonds op zoek is naar innovatie. Andersom kan de situatie zich voordoen dat het fonds na jaren van verandering toe is aan een stabiele (IT-)dienstverlening met focus op kostenreductie, terwijl de uitvoeringspartner besluit een groot veranderprogramma door te voeren waarbij hij kritieke onderdelen van zijn informatievoorziening in de cloud gaat onderbrengen.

1 In haar toezichtsaanpak (FOCUS) onderkent toezichthouder DNB in haar risicoanalyse infrastructuur & IT als een risk driver. In haar jaarplan 2020 wordt de impact van digitalisering op de operationele bedrijfsvoering en de beheersing van cyberrisico's expliciet benoemd.

Het fonds dient zich dus bewust te zijn van de kwaliteit van de IT-functie van zijn uitvoeringspartner en van diens plannen, teneinde de impact hiervan op zijn eigen strategie en doelstellingen te kunnen inschatten en managen. Andersom geldt dat het fonds bij zijn strategische plannenmakerij niet om de rol van IT heen kan. De kansen en bedreigingen van IT moeten worden betrokken in de strategische planning. Dit kan van invloed zijn op de dienstverlening die het fonds verwacht van zijn uitvoeringspartners.

Steeds minder invloed

De laatste jaren wordt steeds duidelijker dat de besluitvorming over IT-ontwikkelingen in toenemende mate plaatsvindt vanuit het perspectief van de pensioenuitvoerder; pensioenfondsen kunnen daar steeds minder invloed op uitoefenen. In 2016 kondigde Syntrus Achmea aan te stoppen met haar dienstverlening aan bedrijfstakpensioenfondsen en zich primair te richten op ondernemings- en beroepspensioenfondsen.[2] En in 2018 kondigde TKP een meerjarig verandertraject aan, waarbij naast het opzetten van een digitaal pensioenplatform ook een organisatorische aanpassing plaatsvindt om zo de digitale en technologische verandering te kunnen blijven beheersen.[3] In beide voorbeelden leidde de besluitvorming van de pensioenuitvoerder tot het opzeggen van zijn dienstverlening aan een aantal pensioenfondsen, die vervolgens op zoek moe(s)ten naar een geschikte nieuwe pensioenuitvoerder.

Tegelijkertijd moeten bestaande klanten de veranderingen bij hun uitvoerders zien te doorgronden en verwerken in hun eigen risicohouding en in de governance en monitoring van de uitbestedingsrelatie. Hoe dan ook, in alle gevallen geldt dat het fondsbestuur altijd een eigen verantwoordelijkheid heeft (gehad) in de uitbestedingsrelatie. Het kan niet alleen maar vertrouwen op zijn uitbestedingspartner, maar moet in staat zijn effectief tegenwicht te bieden aan professionele uitvoerders.

CYBERSECURITY OP DE BESTUURSAGENDA?

De toegenomen digitalisering en complexere uitbestedingsketens van pensioenfondsen maakt dat veel fondsen cybersecurity als integraal onderdeel van de informatiebeveiliging zijn gaan beschouwen. Ze staan er dan ook steeds nadrukkelijker bij stil, bijvoorbeeld door cyberrisico's expliciet te benoemen en te plaatsen binnen de risicohouding van het fonds. Cyberrisico's kunnen bij het pensioenfonds zelf manifest worden, maar zich ook verderop in de (IT-)keten voordoen. Pensioenfondsen moeten vaststellen of ze zelf adequate maatregelen hebben getroffen – zoals het periodiek houden van awareness trainingen op het gebied van cyberrisico's – of hun ketenpartners bevragen op dit onderdeel.

Voor een goed beeld van actuele, reële cyberrisico's vormt de website van het Nationaal Cyber Security Centrum (NCSC) een waardevolle informatiebron. Het NCSC analyseert de belangrijkste ontwikkelingen op het gebied van digitale veiligheid en geeft duiding aan actuele ontwikkelingen. Op zijn website (www.ncsc.nl) publiceert het een tijdslijn waarop per maand de meest relevante gebeurtenissen worden samengevat. Ook stelt toezichthouder DNB zwaardere eisen aan de beheersing van het cyberrisico door pensioenfondsen. In het voorjaar van 2019 heeft ze haar Good Practice Informatiebeveiliging geactualiseerd. Naast het toevoegen van specifieke maatregelen voor cyberrisico's wordt meer aandacht besteed aan de beheersing van cyberrisico's en aan informatiebeveiliging bij uitbesteding en onderuitbesteding. Ook veronderstelt DNB dat pensioenfondsen aantoonbaar 'in control' zijn op het gebied van informatiebeveiliging en cybersecurity.

IN VIER STAPPEN NAAR EIGEN REGIE

Om als fondsbestuur(der) de eigen verantwoordelijkheid te dragen voor de beheersing van de IT-risico's in de uitbestedingsrelatie is het van belang zelf regie te pakken. De aard van de bestuursfunctie, alsook de organisatie van pensioenfondsen schreeuwt hierbij om een pragmatische benadering. Wij hebben daarom een aanpak ontwikkeld om vanaf de bestuurstafel in vier stappen 'in control' te komen over de IT-functie in de uitbestedingsketen:

> De besluitvorming over IT-ontwikkelingen vindt in toenemende mate plaats vanuit het perspectief van de pensioenuitvoerder

1. dicht de kloof tussen 'business' en de IT-functie via meer aandacht en bewustzijn bij de fondsbestuurder voor het belang van een brugfunctie;
2. zorg voor sturing op de IT-functie, met IT-governance en principes die richtinggevend zijn voor het uitoefenen van de IT-functie ten dienste van het fonds;
3. zorg voor focus en blijf deze scherpstellen, zodat de juiste onderwerpen de aandacht krijgen;
4. zorg voor stevig fundament, door aansluiting te zoeken bij bestaande structuren en methoden van het fonds.

Stap 1: Dicht de kloof tussen business en de IT-functie

De vraag hoe het pensioenfonds IT-beheersing op de meest passende wijze kan vormgeven wordt voorafgegaan door een meer fundamentele vraag. Namelijk de vraag of het bestuur IT beschouwt als een noodzakelijk kwaad (*facilitator*) of als een middel om de doelstellingen van het fonds te realiseren (*enabler*). Het omarmen van het begrip *strategic alignment* – de mate waarin IT de doelstellingen van het fonds helpt te realiseren en de procesuitvoering ondersteunt – geldt als een onmisbare randvoorwaarde voor het dichten van de kloof tussen de verwachtingen van de 'business' en de prestaties van de IT-functie.

De risicoanalyse is een geschikt instrument om het belang van IT voor het fonds zichtbaar te maken. Door hierin de vier 'A's' in relatie tot de (uitbestede) processen van het fonds centraal te stellen, wordt een inschatting gemaakt van de gevolgen van IT-risico's (zie kader). Een belangrijk onderdeel is het in kaart brengen van het op fondsniveau aanwezige inzicht in de omvang en complexiteit van de IT-keten. De risicoanalyse geeft hiermee richting aan de sturing op de IT-functie vanuit het perspectief van het fonds.
Door het creëren van bestuurlijke betrokkenheid bij de uitvoering van de IT-risicoanalyse wordt geïnvesteerd in bewustzijn, oftewel de vijfde 'A' (Awareness). Bewustzijn van het feit dat IT een aandachtsgebied van het bestuur zelf is, maar ook dat het bestuur zelf in staat is keuzes te maken, en wellicht belangrijker, dat deze keuzes simpelweg niet alleen aan de uitvoeringsorganisatie mogen worden overgelaten.

Stap 2: Zorg voor sturing op de IT-functie

Het beleggen van taken en verantwoordelijkheden in het bestuur – of bij het bestuursbureau – is noodzakelijk om het IT-beleid en de uitvoering daarvan onderdeel te maken van het perspectief van de bestuurder. Om dat voor elkaar te krijgen is binnen het bestuur begrip en draagvlak nodig voor IT-onderwerpen. Het uitvoeren van de IT-risicoanalyse met bestuurlijke betrokkenheid (stap 1) draagt bij aan deze bewustwording.
Daarnaast moet niet worden geschroomd om te investeren in voldoende kennis en communicatieve vaardigheden op het gebied van IT en informatiemanagement. Het beschikken over voldoende *countervailing power* betaalt zich terug: IT komt van zijn eiland en indien goed uitgevoerd ervaart het fonds toegevoegde waarde.
Het is van belang dat fondsbestuurders onderkennen dat IT de verantwoordelijkheid is van het pensioenfonds en niet (enkel) van de uitvoeringsorganisatie. Daartoe moet deze verantwoordelijkheid eenduidig binnen het fonds worden belegd. De eerste stap hiertoe is vaststellen wie binnen het fonds primair verantwoordelijk is voor het onderwerp IT en daarbij over voldoende kennis beschikt. Kwetsbaarheid is hierbij kracht, door met een zelfkritische blik vast te stellen of die kennis in voldoende mate aanwezig is.
Afhankelijk van de omvang van het fonds kunnen taken worden gedelegeerd naar daartoe ingestelde commissies, al dan niet ondersteund door een bestuursbureau. Dat is niet alleen wenselijk vanuit oogpunt van werkverdeling, maar ook met het oog op de aanwezige kennis van processen en bijzonderheden ten aanzien van het desbetreffende IT-domein. Zo zijn in een beleggingscommissie doorgaans die bestuursleden en fondsmedewerkers vertegenwoordigd die kennis hebben van de processen van vermogensbeheer. Ook beschikken deze commissieleden veelal over de contacten met de relevante uitvoeringsorganisaties. Bij grotere fondsen kan dan het onderscheid worden gemaakt tussen besturen en besluiten: het bestuur bestuurt, terwijl besluiten door commissies binnen geldende beleidskaders worden genomen.
Het vaststellen en communiceren van IT-principes geldt als een onmisbaar instrument voor het pensioenfonds om vanaf de bestuurstafel regie te voeren over de IT-functie. Regie om de voordelen van samenwerking en uitbesteding te realiseren zonder de controle kwijt te raken. Ze maken duidelijk hoe door het fondsbestuur wordt gedacht over de IT-functie. Daarnaast zorgen de principes ervoor dat vanuit verschillende perspectieven (fonds en uitvoerder) in eenzelfde taal met elkaar wordt gesproken over IT. Verder zorgen ze voor een voorspelbaarder inrichting en functioneren van de IT-functie van de uitvoeringsorganisatie, mits goed overeengekomen met en nageleefd door de uitvoeringsorganisatie. Tot slot zijn de principes richtinggevend voor het monitoren van de aan de uitvoeringsorganisatie uitbestede IT-functie.[4]
Van belang is voorts dat het pensioenfonds oog heeft voor relevante ontwikkelingen op het gebied van IT, ook als die zich voornamelijk bij de uitvoeringspartner en diens ketenpartners voordoen. Dit kunnen ontwikkelingen op technologisch vlak zijn, maar ook ontwikkelingen binnen de pensioensector, bij uitvoeringspartners en zelfs binnen het eigen fonds. Door hier bewust aandacht aan te besteden, al dan niet begeleid door externe deskundigen, zorgt het fondsbestuur voor gedachtevorming op het gebied van IT en

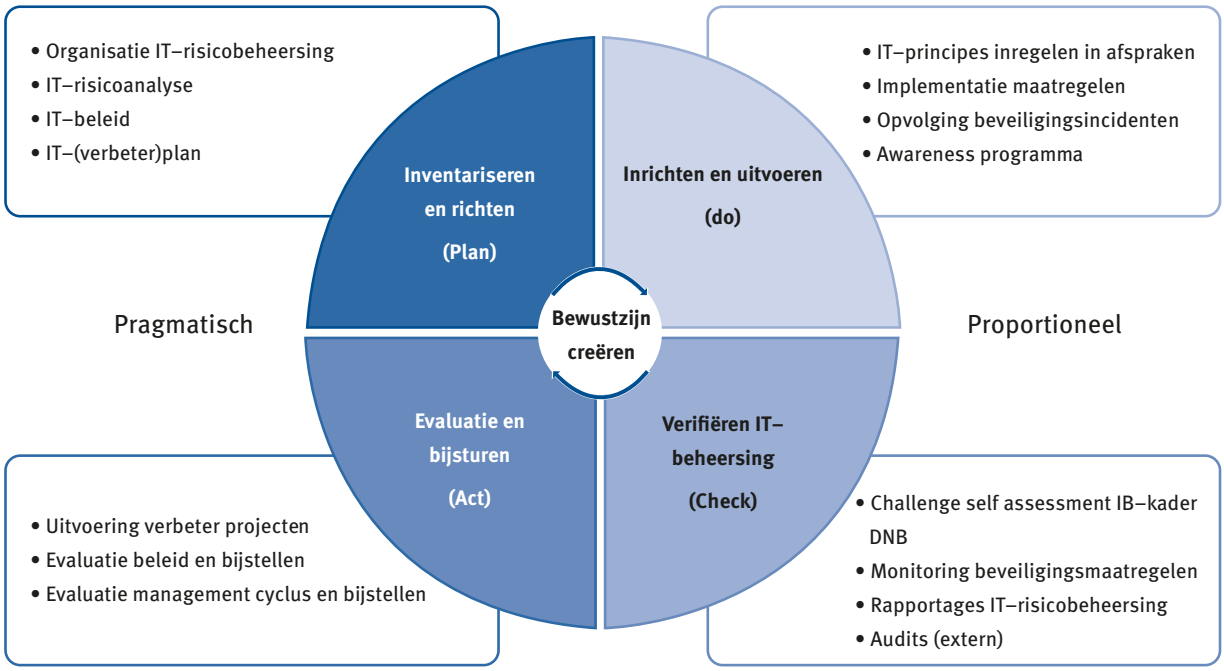
De vijf A's van het IT-risico

DNB hanteert de volgende aandachtsgebieden (de vier A's) voor het behandelen van de IT-risico's voor de eigen bestuursomgeving van het fonds, voor de uitvoerder van de rechtenadministratie en voor de uitvoerder van het vermogensbeheer:
- *Availability* (beschikbaarheid): het draaiend houden van bestaande processen en het herstellen van verstoringen, waarbij de negatieve gevolgen van incidenten, zoals uitval en beveiligingslekken, worden beperkt;
- *Access* (toegang): waarborgen dat de juiste mensen toegang hebben tot de juiste informatie en anderen niet;
- *Accuracy* (integriteit): opleveren van juiste, tijdige en volledige informatie aan alle relevante belanghebbenden;
- *Agility* (aanpasbaarheid): ondersteunen van veranderingen in de bedrijfsvoering als gevolg van interne en externe oorzaken tegen acceptabele kosten en binnen acceptabele tijd.

De Pensioenfederatie heeft hier een vijfde A aan toegevoegd:
- *Awareness* (bewustzijn): het begrijpen van het belang van IT-beheersing en het naleven van IT- en informatiebeveiligingsrichtlijnen door alle betrokkenen.

2 Syntrus Achmea: https://www.findinet.nl/persbericht/syntrus-achmea-stopt-met-bedrijfstakpensioenfondsen/
3 TKP: https://www.tkppensioen.nl/expertise/nu-is-het-moment-voor-de-cloud
4 De Good Practice informatiebeveiliging van DNB biedt handvatten voor het identificeren van belangrijke onderwerpen waarvoor principes moeten worden uitgewerkt.

Figuur 1. Managementcyclus beheersing IT-functie



daarmee voor meer bewustzijn, alsook voor gesprekstof voor het overleg met de uitvoeringspartner.

Stap 3: Zorg voor focus en blijf scherpstellen

Het is van belang om de toegevoegde waarde van de IT-functie op het vereiste niveau te brengen en daar ook op te houden. Toezichthouder DNB verwacht van het fonds dat het de effectiviteit kan aantonen van de maatregelen die het op dit vlak dient te treffen. Op het gebied van IT Risk Management wordt verwacht dat die effectiviteit periodiek wordt beoordeeld en waar nodig verbeterd. Door het opzetten van een continue managementcyclus voor beheersing van de IT-functie kan het fonds steeds de focus bepalen en waar nodig scherpstellen; zie figuur 1.

Het pensioenfonds dient oog te hebben voor relevante ontwikkelingen op het gebied van IT, ook als die zich voornamelijk bij de uitvoeringspartner voordoen

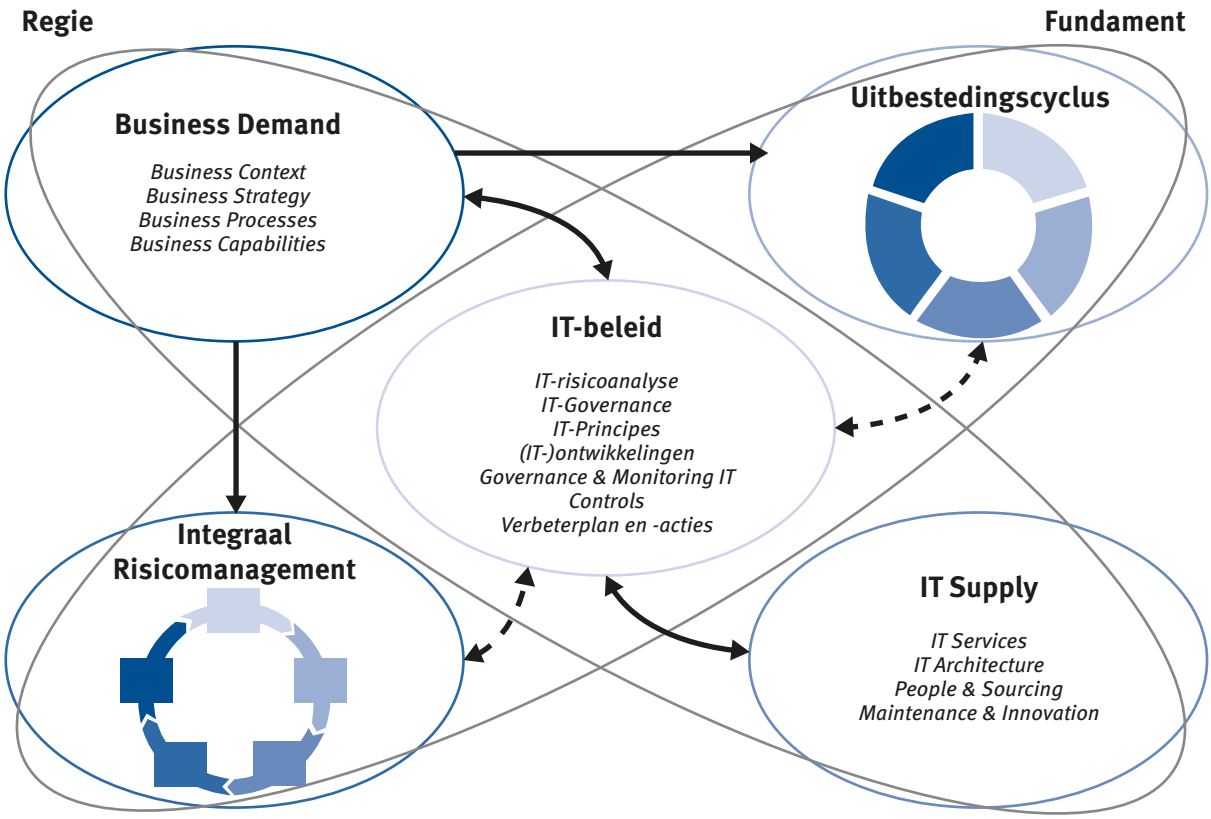
Bij dit proces van continue verbetering geldt het adagium dat niet alles tegelijk kan worden gedaan. De uitkomsten van de IT-risicoanalyse en het verkregen inzicht in de IT-keten – of het gebrek daaraan – helpen het fonds bij het identificeren van verbeteracties en het maken van keuzes. Ook de beoordelingen van service level rapportages, audit rapporten en andere verantwoordingsinformatie gelden als belangrijke instrumenten om te focussen en scherp te stellen. Aard en diepgang van de verantwoordingsinformatie worden door het fonds afgestemd op het belang van de IT-functie, bijvoorbeeld aan de hand van de te beheersen risico's. Dit proportionaliteitsbeginsel is essentieel voor het op pragmatische en kostenefficiënte wijze vormgeven van sturing op de IT-functie. Door het werken met een duidelijk IT-verbeterplan of -actielijst worden de besluitvorming, het opvolgen van acties en de voortgangsbewaking zichtbaar gemaakt.

Stap 4: Zorg voor stevig fundament

Het borgen van sturing op de IT-functie en het aanbrengen van focus in IT-beheersing via een continu proces zijn voorwaarden voor het creëren van toegevoegde waarde door de IT-functie. Tegelijk is het van belang dat IT-onderwerpen simpel worden gemaakt, zodat ze aan de bestuurstafel vanuit het juiste perspectief en met de juiste positieve mindset worden behandeld. Een stevig fundament is hiervoor essentieel, waarbij de sleutel tot succes ligt in de verankering van IT-beheersing in de reguliere bedrijfsvoering van het pensioenfonds, in het bijzonder de beleidscycli op het gebied van integraal risicomanagement (IRM) en uitbesteding. Veelal zijn deze processen op een volwassen manier opgezet en geïmplementeerd. Op deze wijze wordt regie op de IT-functie op pragmatische wijze onderdeel van de bedrijfsvoering van het fonds; zie figuur 2.

De drie voorgaande stappen worden binnen de beleidskaders van het fonds op maat uitgewerkt (passend en proportioneel). De integrale risicomanagementmethode kan worden gebruikt om de IT-risicoanalyse van het fonds vorm te geven. Het risicobeoordelingskader wordt dan gebruikt om te bepalen waar prioriteiten moeten worden gelegd (focus). Zo kunnen risico's worden onderkend die volgens de

Figuur 2. Regie op de IT-functie als pragmatisch onderdeel bedrijfsvoering fonds



risicohouding van het fonds onacceptabel zijn en per direct dienen te worden geadresseerd.

Door in de diverse fasen van de uitbestedingscyclus gepaste aandacht aan de IT-functie te besteden, wordt het continue proces van beheersing en verbetering versterkt. Denk hierbij aan het hanteren van IT-principes en de risicoclassificaties als criteria bij de selectie van een uitvoeringspartner. Een en ander gaat eenvoudiger als vooraf duidelijk is dat de maatregelen voor informatiebeveiliging van de uitvoeringspartner passend zijn voor de IT-risicohouding van het fonds. Een logische vervolgstap zou zijn het borgen van de IT-principes in de contractuele afspraken met de uitvoeringspartner. Denk hierbij aan het overeenkomen van een dataclassificatieoverzicht waarin ten minste de risicoaspecten beschikbaarheid, integriteit en vertrouwelijkheid zijn opgenomen. Of het gebruik van specifieke standaarden voor de inrichting en monitoring van maatregelen door de uitvoeringspartner, zoals Cobit en ISO27001. Het behoeft geen uitleg dat met het hanteren van dergelijke selectiecriteria en het overeenkomen van duidelijke afspraken over IT-principes de monitoring van de uitvoeringsrelatie concreet handen en voeten kan worden gegeven.

Tot slot vormt de jaarkalender van het fonds een belangrijk, praktisch onderdeel van het fundament. De activiteiten uit de managementcyclus IT-beheersing en de uitvoering van beheersmaatregelen worden opgenomen in de jaarkalender. Denk hierbij aan IT als onderdeel van de commissievergaderingen en specifieke IT-aspecten als onderdeel van de beoordeling van assurancerapportages, zoals de mate waarin IT voldoende in scope is van het rapport. Op deze wijze wordt tijdigheid van uitvoering van maatregelen geborgd, alsook invulling gegeven aan taken en verantwoordelijkheden.

CONCLUSIE

Door de verdergaande oprekking van de IT-ketens, technologische innovaties en legacyproblemen is de IT-functie steeds verder van de bestuurstafel af komen te staan. De brugfunctie tussen het pensioenfonds en de IT-functie van de uitvoerder verdient aandacht. Daarvoor is bewustwording en kwetsbaarheid bij de bestuurder nodig: het belang inzien, de verantwoordelijkheid durven pakken en op de juiste momenten deskundige hulp inschakelen.

Ook moet het pensioenfonds meer sturing geven aan de IT-functie: wie stuurt en wie besluit over IT hoeven niet dezelfde te zijn. Zolang de IT-governancestructuur goed in elkaar steekt, is dit geen probleem. Het gebruik van principes en het identificeren van relevante ontwikkelingen helpt om de verwachtingen te managen en duidelijk sturing te geven aan de inrichting, beveiliging en beheersing van de IT-functie. Focus is daarbij van belang: wat zijn de belangrijkste acties voor het fonds om de IT-functie blijvend op niveau te houden of te krijgen. Door ten slotte aansluiting te vinden bij bestaande structuren en methoden binnen het fonds, zoals de risicomanagementaanpak en de implementatie van de uitbestedingscyclus, wordt de regie op de IT-functie verankerd binnen bestaande werkwijzen van het fonds. Door de vier beschreven stappen te doorlopen kunnen pensioenfondsen op pragmatische wijze regie pakken op de inrichting, beveiliging en beheersing van hun IT-functie.