SPO pensioenopleiders

Leergang IT Governance

Resultaten

continu in ontwikkeling

Module IT Governance, inrichting & change

Na afronding van deze module kunt u:

- Het systeemlandschap van het pensioenfonds en de uitvoerder schetsen en toelichten vanuit gangbare standaarden in IT-architectuur
- Toelichten wat verstaan wordt onder IT-inrichting, welke plaats de IT-architectuur inneemt en het werkgebied van de IT-architect omschrijven
- Belangrijke veranderingen in de IT-architectuur benoemen en de gevolgen ervan duiden, alsmede hoe een pensioenfonds hierop kan inspringen
- Een overzicht geven van de verdeling van taken, bevoegdheden en verantwoordelijkheden van de IT-governance in een pensioenfonds, inclusief de verdeling tussen bestuur en uitbestedingspartijen
- Cloud computing: karakteriseren van de werking/ gevaren / voordelen/ toepassing van de cloud
- Beschrijven welke invloed een IT-inrichting heeft op de wendbaarheid en het verandervermogen van uw eigen pensioenfonds

Module IT risico’s & trends

Na afronding van deze module kunt u:

- Uitleggen welke stappen te doorlopen om invulling te geven aan IT-risicomanagement
- Een analyse geven van de risico's in IT-gebruik van het eigen fonds (gedrag van zichzelf, bestuur als geheel en bestuursbureau)
- IT-risico's op het gebied van informatiebeveiliging onderscheiden van risico’s in de doorontwikkeling van de informatievoorziening
- Ongewenste functievermengingen (toxic combinations) herkennen en de bijbehorende risico's toelichten
- Afhankelijkheden van IT voor het pensioenfonds op kernprocessen beschrijven en zwakke plekke benoemen
- De risicomanagementcyclus toelichten vanuit IT-oogpunt
- Innovatieve IT-toepassingen binnen de Nederlandse pensioenmarkt benoemen en de mogelijkheden en kansen toelichten vanuit resultaten bij andere pensioenfondsen
- Kansrijke IT-ontwikkelingen uit andere sectoren benoemen en de impact op de pensioensector toelichten
- Opkomende IT-innovaties beknopt toelichten (vergezicht)

Module IT-beleid & uitbesteding

Na afronding van deze module kunt u:

- Beschrijven welke richtinggevende principes kunnen worden meegewogen in het IT-beleid
- Toelichten uit welke data de pensioenadministratie en vermogensbeheer bestaat en typeren wat goede datakwaliteit inhoudt
- De IT-gerelateerde risico's in de uitbestedingsstrategie aanduiden
- Weergeven welke onderwerpen in het eigen beleid rondom datakwaliteit aan de orde moeten komen (risk appetite, kader voor PUO, monitoring etc.)
- Relevante vragen formuleren voor het evalueren van het IT-uitbestedingsbeleid
- Relevantie van een dataclassificatiemodel uitleggen voor het IT-beleid en een toepassing voor uw eigen fonds geven
- Belangrijke richtlijnen voor informatiebeveiliging en rapportages erover beschrijven

Module Informatiebeveiliging & cybersecurity

Na afronding van deze module kunt u:

- De taken en verantwoordelijkheden op het gebied van het inrichten, beheren en controleren van informatiebeveiliging en cybersecurity effectief beleggen
- Een periodiek IT-, uitbestedings- en informatiebeveiligingsbeleid vaststellen, met een actieplan dat aansluit bij het risicokader en eisen uit wet- en regelgeving
- Relevante risico’s op informatiebeveiliging en cybersecurity identificeren, analyseren en toetsen aan de risicobereidheid en acties hieraan koppelen; ook als deze uitbesteed zijn aan derde partijen of risico’s zich bevinden bij een dienstverlener verderop in de uitbestedingsketen
- Naast kritische vragen stellen over informatiebeveiliging en cybersecurity, ook actief bijdragen aan oplossingsrichtingen om de goede strategische en tactische keuzes te maken; bijvoorbeeld in de transitie naar een nieuw pensioensysteem (datakwaliteit en aanpasbaarheid van IT-systemen)
- Het raamwerk van informatiebeveiliging integraal onderdeel maken van het overkoepelende risicoraamwerk en een effectieve evaluatiecyclus opzetten, die leidt tot continue verbeteringen tegen interne en externe dreigingen
- Het bewustzijn over cyberrisico’s in het fonds bevorderen door inzet van trainingsprogramma’s en voorbeeldgedrag, mede gebruikmakend van de 58 beheersmaatregelen uit de Good Practice Informatiebeveiliging (GPIB) van DNB
- Aangeven welke stappen er doorlopen moeten worden in het geval van een incident en/of crisissituatie, zonodig sturing geven aan een respons, toelichten waarop te evalueren nadat een incident zich heeft voorgedaan en leerpunten verwerken in de risicomanagementcyclus
- De jaarlijkse controle van de aansluiting van het IT-continuïteits- en recoveryplan op de (uitbestede) IT-omgeving beschrijven en actief deelnemen aan de periodiek uit te voeren continuïteitstesten en crisisoefeningen

Modules IT & het nieuwe pensioenakkoord

Na afronding van deze module kunt u:

- Beschrijven hoe de IT-governance van uw pensioenfonds is georganiseerd voor inrichting van het nieuwe pensioensysteem (key rollen intern en extern, rol bestuur en VO)
- Valkuilen benoemen vanuit het oogpunt van IT en datakwaliteit voor rechtenbeheer in de transitie naar een nieuw pensioenstelsel
- Datastromen op hoofdlijnen beschrijven voor uw fonds
- Een inschatting geven van de mate waarin uw fonds gereed is om pensioenrechten om te zetten naar een nieuw pensioensysteem
- Het belang en de impact beschrijven van de integratie van de pensioenadministratie en het vermogensbeheer in het IT-landschap
- Beargumenteren hoe de kosten per deelnemer opgebouwd zullen zijn.