Beleidsdocument Informatiebeveiliging 2025

Stichting Bedrijfstakpensioenfonds voor de Betonproductenindustrie

0.5 juli 2025

Stichting Bedrijfstakpensioenfonds
voor de Betonproductenindustrie

Inhoud

1. Inleiding 5
Leeswijzer 5
2. Governance en organisatie 6
2.1 Verantwoordelijkheid bestuur 6
2.1.1 Uitbesteding 6
2.1.2. Governance 7
2.2 Uitvoering informatiebeveiligingsbeleid 8
3. Kader voor ICT-risicobeheer 10
3.1 Definitie 10
3.2 Doelstellingen 10
3.3 Uitgangspunten en strategie 11
3.4 Risicohouding en risicobereidheidsprincipes 12
3.5 Uitbesteding 14
4. Uitvoering van ICT-risicobeheer 16
4.1 Uitwerking beleid 16
4.2 Wet en regelgeving, standaarden en best practices 17
4.3 Identificatie, classificatie en documentatie 18
4.3.1 BIV-analyse 18
4.3.2 Beschikbaarheid 18
4.3.2 Integriteit 18
4.3.3 Vertrouwelijkheid 18
4.4 Mensen (People) 19
4.4.1 Bestuur en personeel 19
4.4.2 Bewustzijn, opleiding en training 19
4.4.3 Sancties 19
4.4.4 Beëindiging bestuurderschap of het dienstverband 20
4.5.1 Melden van (beveiligings)incidenten 20
4.5.2 Bedrijfsmiddelen 20
4.5.3 Opslag van informatie 20
4.5.4 Printen van informatie 21
4.5.5 Verstrekken van informatie 21
4.5.6 Verstrekken van fondsinformatie 21
4.5.7 Verwijderen en vernietigen van informatie 21
4.5.8 Bewaartermijnen 21
4.5.9 Wijzigingsbeheer 22
4.5.10 Scheiding Ontwikkel-Test-Productie-omgevingen 22
4.5.11 Leveranciersrelaties 22

4.5.12 Continuïteit management 22
4.5.13 Business Impact Analyse 22
4.5.14 Business Continuity Plan 23
4.5.15 Uitwijkvoorziening 23
4.5.16 Back-up en recovery 23
4.6.1 Autorisatie 23
4.6.2 Wachtwoorden 23
4.6.3 Toegang via (mobiele) devices 23
4.6.4 Externe toegang 23
4.6.5 Authenticatie 24
4.6.6 High privileged accounts 24
4.6.7 Cryptografie 24
4.6.8 Opslag op digitale media 24
4.6.9 Bestanden 24
4.6.10 Databases 24
4.6.11 E-mail 24
4.6.12 Beheersmaatregelen tegen malware 24
4.6.13 Communicatiebeveiliging 25
4.6.14 Het beheer van de netwerkbeveiliging 25
4.6.15 Scheiding in netwerken 25
4.7 Faciliteiten 25
4.7.1 Clouddiensten 25
4.7.2 Fysieke beveiliging en beveiliging van de omgeving 25
4.7.3 Algemene toegang 25
4.8 Uitbesteding 25
4.9 (Security) Testing 26
4.10 (Risicomanagement) Proces 26
Plan 27
Do 27
Check 28
Act 28
4.11 Risicobeheersing 28
4.11.1 ICT-gerelateerde incidenten 28
4.11.2 Datalek 29
5. Inbedding in integraal risicomanagement 30
6. Informatie-uitwisseling 30
7. Verantwoording 30
8. Bekendmaking beleid 31

9. Inwerkingtreding beleid 31
Bijlage 1 – BIV-classificatie 32
Bijlage 2 - DNB Toetsingskader Informatiebeveiliging 2023 34
Bijlage 3 – controles DORA artikel 9 tot en met 14 36
Eenmalige, periodiek te herhalen controles 36
Controles op basis van regelmatige rapportages 40

1. Inleiding

Financiële entiteiten beschikken over een intern governance- en controlekader dat een doeltreffend en prudent beheer van het ICT-risico waarborgt, teneinde een hoog niveau van digitale operationele weerbaarheid te verkrijgen. Dit Beleidsdocument informatiebeveiligingsbeleid is de vastlegging van dit kader voor het Bedrijfstakpensioenfonds voor de Betonproductenindustrie (hierna: BPF Beton).

Informatiebeveiliging is heden ten dage een van de belangrijkste aandachtspunten voor BPF Beton mede in het kader van een beheerste en integere bedrijfsvoering. Derhalve heeft het bestuur in 2021 beleid over informatiebeveiliging geformuleerd en vastgelegd in het eerdere Beleidsdocument informatiebeveiliging (december 2021). Dit beleid vormt het uitgangspunt voor de maatregelen die waarborgen dat BPF Beton en haar uitbestedingsrelaties voldoen aan geldende normen ('best practices') en wet- en regelgeving. Het pensioenfonds blijft te allen tijde verantwoordelijk voor de beheersing van informatiebeveiligingsrisico's, ook voor de uitbestede werkzaamheden.

Informatiebeveiliging draagt bij aan een veilige werkomgeving en schept vertrouwen bij de belanghebbenden van BPF Beton. Zij mogen er op vertrouwen dat het pensioenfonds informatie beveiligt en dezelfde eisen stelt aan haar uitbestedingsrelaties.

Per 17 januari 2025 is de Digital Operations Resilience Act (DORA) van kracht geworden. Deze Europese verordening schrijft voor hoe financiële instellingen zoals BPF Beton hun digitale weerbaarheid dienen vorm te geven en vast te leggen. Het bestuur heeft een inventarisatie gemaakt van de vereisten op grond waarvan het Beleidsdocument informatiebeveiliging geactualiseerd moet worden. Deze nieuwe versie van het Beleidsdocument informatiebeveiligingsbeleid is daarvan de weerslag, waarbij de indeling in lijn is gebracht met DORA.

De belangrijkste ICT-systemen van BPF Beton zijn in beheer bij de uitbestedingsrelaties. Primair ligt de verantwoordelijkheid voor de uitvoering van het grootste deel van de DORA-vereisten daarom bij die organisaties. BPF Beton blijft echter eindverantwoordelijke. De nadruk voor deze verordening voor BPF Beton ligt daardoor op het toezien op of en hoe de uitbestedingsrelaties aan die vereisten voldoen.

Van de uitbestedingsrelaties is Appel Pensioenuitvoering eveneens gebonden aan de DORA-voorschriften. Het toezicht op de digitale weerbaarheid kan in dit geval worden uitgevoerd door controle op de naleving daarvan door Appel. De andere uitbestedingsrelaties voor wie de digitale weerbaarheid van belang is voor BPF Beton – met name de custodian en de vermogensbeheerders –, zijn geen ICT-dienstverleners maar zijn zelf wel DORA-plichtig.

Leeswijzer

Dit document is als volgt opgebouwd. In hoofdstuk 2 wordt de governance en de organisatie beschreven ten aanzien van de uitvoering van dit informatiebeveiligingsbeleid. In hoofdstuk 3 is het strategische kader van informatiebeveiliging opgenomen zoals dat door het bestuur in lijn met de missie, visie en strategie is uitgewerkt en vastgesteld. Hoofdstuk 4 beschrijft het inhoudelijke beleid. Vervolgens beschrijft hoofdstuk 5 de wijze waarop het informatiebeveiligingsbeleid onderdeel is van het integraal risicomanagement en wordt het jaarlijks te doorlopen proces beschreven. In hoofdstuk 6 wordt beschreven dat het bestuur verantwoording aflegt over de uitkomsten van het gevoerde beleid en aan welke partijen. Hoofdstuk 7 beschrijft de periodieke publicatie van het beleid en hoofdstuk 8 wordt tenslotte vermeld wanneer dit beleidsdocument voor het laatst is gewijzigd en vastgesteld.

2. Governance en organisatie

Dit beleid beschrijft de informatiebeveiliging van BPF Beton en op wie[1] het van toepassing is. In beginsel zijn dat het bestuur en de organen van het pensioenfonds (het verantwoordingsorgaan en de raad van toezicht) en alle uitbestedingsrelaties die werkzaam zijn voor het pensioenfonds.

Kennis van informatiebeveiliging binnen het bestuur is belangrijk. Periodiek beoordeelt het bestuur of er voldoende kennis binnen het bestuur aanwezig is om de risico's goed in te schatten en om voldoende 'countervailing power' te leveren tegenover de uitbestedingspartners van het fonds. De onafhankelijk bestuurder risicomanagement vervult sec deze rol als onderdeel van het bestuur en is portefeuillehouder. Het bestuur heeft Sprenkels belast met het sleutelfunctiehouderschap risicomanagement. Het bestuur is zich er van bewust dat specialistische kennis van tijd tot tijd nodig zou kunnen zijn en zal deze specialistische kennis zo nodig extern inhuren.

Het bestuur stelt een Chief Information Security Officer (CISO) aan. De CISO is namens het bestuur verantwoordelijk voor het toezicht op het ICT-risicomanagement en op het voldoen aan de wet- en regelgeving, waaronder DORA. De CISO rapporteert regelmatig en indien nodig incidenteel aan het bestuur, signaleert ontwikkelingen ten aanzien van ICT-risico's en wet- en regelgeving en doet voorstellen om hierop te anticiperen.

2.1 Verantwoordelijkheid bestuur

Het bestuur is eindverantwoordelijk voor het beheer van het ICT-risico van het fonds. Dit hoofdstuk beschrijft welke verantwoordelijkheden dit betreft. Per verantwoordelijkheid wordt voor de vormgeving en uitwerking van het beleid verwezen naar latere hoofdstukken in dit beleidsdocument.

2.1.1 Uitbesteding

Het pensioenfonds heeft de voornaamste processen uitbesteed aan externe partijen. Dat betekent dat ook de belangrijkste risico's daar liggen alsmede in de afstemming tussen en met de externe partijen. De nadruk van het ICT-risicobeheer ligt daarom in het monitoren van het risicobeheer door de externe partijen.

Het pensioenfonds hanteert als voorwaarde voor uitbestedingsrelaties dat zij voldoen aan het informatiebeveiligingsbeleid van het fonds en beschikken over eigen beleid dat minimaal gelijkwaardig is aan het beleid dat BPF Beton hanteert. BPF Beton evalueert periodiek, indien daartoe aanleiding bestaat, of de uitbestedingsrelaties voldoen aan de regels van dit informatiebeveiligingsbeleid. Een audit kan onderdeel gaan uitmaken van de monitoring. BPF Beton zal tenminste toetsen of de uitbestedingspartij voldoet aan de door DORA gestelde eisen.

Het bestuur houdt bij de aangestelde uitbestedingspartijen zicht op de strategische (wijzigingen in) IT-infrastructuur, de IT-processen, dataverwerking, -opslag en -beveiliging en beoordeelt tevens of de uitbestedingspartij voldoet aan de geldende wet- en regelgeving.

Het bestuur meldt 'belangrijke of kritieke activiteiten' van een (onder)uitbesteding aan DNB. Belangrijke of kritieke activiteiten hebben betrekking op de pensioenadministratie (rechtenbeheer/excasso van pensioenbetalingen) en het (fiduciair) vermogensbeheer van tenminste 30% van het balanstotaal.

Persoonsgegevens van het fonds, die door de (onder)uitbestedingspartij worden verwerkt,

[1] Voor een volledige beschrijving van de governance verwijzen wij u naar paragraaf 1.2 van de Actuariële en bedrijfstechnische nota (Abtn)

worden idealiter in Nederland verwerkt en bewaard of hooguit in de Europese Unie opgeslagen maar zeker niet buiten de Europese Unie.

2.1.2. Governance

Het bestuur bepaalt de reikwijdte van het ICT-risicobeheer. Het streeft naar een hoge mate van beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de gegevens. Daartoe voort het bestuur de beleidslijnen op die in dit document zijn opgenomen, stelt het de strategie vast voor digitale operationele weerbaarheid en bepaalt daarbij het passende risicotolerantieniveau voor het ICT-risico.

Het bestuur zorgt voor een adequate organisatie van duidelijke taken, verantwoordelijkheden en bevoegdheden voor alle ICT-gerelateerde functies en van passende governanceregelingen om te zorgen voor doeltreffende en tijdige communicatie, samenwerking en coördinatie tussen die functies. Vanwege de hoge mate van uitbesteding betekent dit vooral het toezicht op de uitbestedingspartijen. Het bestuur heeft hier de IRM-commissie mee belast. In hoofdstuk 2.3 wordt nader ingegaan op de taken van de IRM-commissie.

Het bestuur ziet erop toe dat alle elementen van informatiebeveiliging en cybersecurity zijn beheerst. De taken en verantwoordelijkheden op het gebied van het inrichten, beheren en controleren van informatiebeveiliging en cybersecurity zijn belegd bij de IRM-commissie. Het bestuur zorgt ervoor dat deze over voldoende capaciteit, kennis en ervaring beschikt om invulling te geven aan deze taken en verantwoordelijkheden.

Het bestuur en de commissie dragen actief en zichtbaar het belang uit van informatiebeveiliging en cybersecurity voor BPF Beton, in het bijzonder jegens de uitbestedingspartijen. De IRM-commissie controleert actief op het nakomen van de gemaakte afspraken over het beleggen van taken en verantwoordelijkheden voor informatiebeveiliging en cybersecurity, eigenaarschap van gegevens en informatiesystemen en functiescheiding bij deze partijen.

Het bestuur is belast met de goedkeuring van, het toezicht op en de periodieke evaluatie van de uitvoering van het beleid inzake ICT-bedrijfscontinuïteit en van de ICT-respons- en herstelplannen van het fonds. Het houdt toezicht op de uitvoering van het informatiebeveiligingsbeleid door de IRM-commissie en is ervoor verantwoordelijk.

Het bestuur is belast met de goedkeuring en de periodieke evaluatie van de interne ICT-auditplannen en ICT-audits van het fonds en materiële wijzigingen daarvan.

Het bestuur is belast met de toewijzing en de periodieke evaluatie van het passende budget om te voldoen aan de behoeften inzake digitale operationele weerbaarheid van het fonds. Daaronder vallen alle soorten middelen, waaronder relevante bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid en ICT-vaardigheden voor alle medewerkers en bestuursleden.

Het bestuur is belast met de goedkeuring en de periodieke evaluatie van het beleid van het fonds inzake regelingen betreffende het gebruik van ICT-diensten die door derde aanbieders van ICT-diensten worden verleend.

De bestuursleden onderhouden actief voldoende kennis en vaardigheden om ICT-risico en de gevolgen daarvan voor de verrichtingen van het fonds te begrijpen en te beoordelen, onder meer door regelmatig specifieke opleidingen te volgen die in verhouding staan tot het te beheren ICT-risico.

Het bestuur evalueert het kader voor ICT-risicobeheer jaarlijks, maar ook wanneer zich ernstige ICT-gerelateerde incidenten voordoen en na toezichtinstructies of -conclusies uit relevante tests

of auditprocessen. Het kader wordt voortdurend verbeterd op basis van de lessen die uit de uitvoering en de monitoring naar voren komen.

Het bestuur evalueert jaarlijks en indien nodig of alle door ICT ondersteunde bedrijfsfuncties, taken en verantwoordelijkheden, de informatie- en ICT-activa die deze functies ondersteunen, en hun taken en afhankelijkheden met betrekking tot ICT-risico's naar behoren geïdentificeerd, geclassificeerd en adequaat gedocumenteerd zijn.

Indien aanwezig wordt specifiek voor alle legacy-ICT-systemen het ICT-risico beoordeeld. Dat gebeurt jaarlijks en voor en na de aansluiting van technologieën, toepassingen of systemen.

Het bestuur evalueert jaarlijks de risicoscenario's die op het fonds van invloed zijn.

Het bestuur geeft regelmatig opdracht tot een interne audit door auditors, in overeenstemming met het auditplan van het fonds, op het kader voor ICT-risicobeheer. Deze auditors dienen te beschikken over voldoende kennis, vaardigheden en deskundigheid op het gebied van ICT-risico en over de nodige onafhankelijkheid. De frequentie en de focus van de ICT-audits staan in verhouding tot het ICT-risico van het fonds.

De conclusies van de interne audit worden besproken in het bestuur. Het bestuur bepaalt of en welke acties benodigd zijn, in ieder geval ten aanzien van de kritieke bevindingen, geeft hiertoe opdracht en monitort de opvolging.

Het bestuur verricht een risicobeoordeling bij elke belangrijke wijziging in de netwerk- en informatiesysteeminfrastructuur en in de processen of procedures die van invloed zijn op de door ICT ondersteunde bedrijfsfuncties en informatie- of ICT-activa.

2.2 Uitvoering informatiebeveiligingsbeleid

BPF Beton heeft voor het integrale risicomanagement een IRM-commissie ingesteld onder voorzitterschap van de portefeuillehouder risicobeheer. Het bestuur heeft de uitvoering van het informatiebeveiligingsbeleid neergelegd bij de IRM-commissie. De IRM-commissie beheert het ICT-risico en houdt er toezicht op. Ook beoordeelt zij het functioneren van de CISO. Doordat de grootste risico's bij de uitbestedingsrelaties liggen, is de onafhankelijkheid van de controlefunctie gewaarborgd.

- De IRM-commissie bereidt de werkzaamheden van het bestuur voor de in 2.1 genoemde verantwoordelijkheden voor. Onder meer verzorgt zij een programma waarmee de bestuursleden voldoende kennis en vaardigheden inzake het ICT-risico hebben en houden.

- De IRM-commissie evalueert jaarlijks de informatiebeveiligingsmaatregelen en beoordeelt of de gestelde doelen zijn bereikt. Daarover rapporteert de IRM-commissie aan het bestuur van het pensioenfonds.

- Jaarlijks beoordeelt de IRM-commissie of het informatiebeveiligingsbeleid (fondsbreed) nog adequaat is respectievelijk aanpassing vergt.

- Tevens voert de IRM-commissie periodiek een risicoanalyse uit. De uitkomst van de risicobeoordeling wordt met het bestuur gedeeld.

- De IRM-commissie onderhoudt de contacten en wint informatie in over:
  1) overeenkomsten met derde aanbieders van ICT-diensten inzake het gebruik van ICT-diensten;
  2) elke relevante gepland materiële wijziging betreffende de derde aanbieders van ICT-

diensten;
3) de potentiële effecten van deze veranderingen voor de kritieke of belangrijke functies die onder die overeenkomsten vallen, inclusief door middel van een samenvatting van de risicoanalyse om het effect te beoordelen van die veranderingen op zijn minst ernstige ICT-gerelateerde incidenten en de gevolgen daarvan, alsook respons-, herstel- en corrigerende maatregelen.

- De IRM-commissie monitort de overeenkomsten met derde aanbieders van ICT-diensten met betrekking tot het gebruik van deze diensten en houdt toezicht op de desbetreffende risicoblootstelling en de relevante documentatie.

- De IRM-commissie brengt ten minste jaarlijks verslag uit bij het bestuur over bevindingen uit:
  - de uitgevoerde tests op de digitale operationele weerbaarheid; hierbij wordt de informatie over penetration tests uit de ISAE 3000A-rapportage van de pensioenuitvoeringsorganisatie gebruikt. Deze rapportage wordt samen met het ISAE 3402 type II rapport ook door de Pensioen- en communicatiecommissie beoordeeld,
  - ICT-gerelateerde incidenten die zich in het reële leven hebben voorgedaan, met name cyberaanvallen,
  - problemen die zich voordoen bij de activering van ICT-bedrijfscontinuïteitsplannen en ICT-respons- en -herstelplannen,
  - relevante informatie die met tegenpartijen wordt uitgewisseld en tijdens toetsingen in het toezicht wordt beoordeeld.

  De IRM-commissie doet daarbij aanbevelingen voor passende herzieningen van relevante onderdelen van het kader voor ICT-risicobeheer.

3. Kader voor ICT-risicobeheer

De uitvoering van de (primaire) diensten van BPF Beton zijn sterk afhankelijk van IT en informatiebeveiliging. Deze afhankelijkheid maakt dat BPF Beton kwetsbaar is voor risico's op het gebied van informatiebeveiliging en technologie. Het bestuur heeft dit onderkend en wil deze risico's adequaat beheersen.
De voortschrijdende ontwikkelingen in IT, digitalisering van processen en communicatie en de toegenomen wet- en regelgeving leiden ertoe dat informatiebeveiliging op strategisch niveau in lijn met de missie, visie en strategie wordt behandeld. Het bestuur heeft het onderstaande strategisch kader uitgewerkt.

3.1 Definitie

In dit beleid wordt onder informatiebeveiliging verstaan het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, vertrouwelijkheid en integriteit van informatie binnen BPF Beton garanderen.

3.2 Doelstellingen

Het doel van informatiebeveiliging is een hoge mate van digitale operationele weerbaarheid. Het is van belang de continuïteit en betrouwbaarheid van de IT, de informatie en de informatievoorziening te waarborgen en de gevolgen van eventuele beveiligingsincidenten tot een acceptabel niveau, de door BPF Beton vastgestelde risicobereidheid, te beperken. Cybersecurity is een integraal onderdeel van de informatiebeveiliging. ICT-risico's dienen snel, efficiënt en zo volledig mogelijk aangepakt te worden.

Dit betekent dat BPF Beton de juiste maatregelen wil nemen om binnen het fonds het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid van data te bereiken en te handhaven en de impact van het ICT-risico te minimaliseren.

- Beschikbaarheid: De uitbestedingsrelatie waarborgt dat de geautoriseerde gebruikers op de juiste momenten tijdig toegang verkrijgen tot de informatie van BPF Beton door middel van relevante bedrijfsmiddelen.
- Integriteit: De informatie van het BPF Beton dient juist en volledig te zijn. De informatie die door BPF Beton en de uitvoeringsorganisaties wordt gebruikt, wordt zoveel mogelijk uit originele bronnen (UPA, UWV, BRP) onttrokken.
- Vertrouwelijkheid: Informatie is alleen toegankelijk voor de bevoegde personen.

Concreet richt het ICT-beleid zich op vijf beheersdoelen:

1. deelnemerdata: behalve juistheid van deelnemersgegevens speelt bijvoorbeeld dat data niet 'op straat' komen te liggen (usb-stick) en dat communicatie zorgvuldig dient te verlopen;
2. pensioendata: aanspraken/rechten deelnemers mogen niet onterecht gewijzigd worden of verloren gaan door aanpassing van systemen of conversie van data;
3. beleggingsportefeuille: waarden mogen niet verloren gaan door bijvoorbeeld onderbreking van de beschikbaarheid van systemen of verlies van data. Juistheid van de transacties moet te allen tijde herleidbaar zijn;
4. geld/middelen op bankrekening: bescherming van waarden. Omvat bijvoorbeeld de betaling voor legitieme verleende diensten en de legitieme uitkering van pensioengelden;
5. besluitvorming en monitoring door bestuur: verkeerde of niet tijdige besluitvorming door gebreken (tijdigheid, juistheid, volledigheid) in door ICT gegenereerde informatie.

3.3 Uitgangspunten en strategie

Awareness en in-control

Het bestuur van BPF Beton geeft richting aan het informatiebeveiliging en IT, is in staat om de uitvoering hiervan te monitoren en is in staat hierover verantwoording af te leggen aan stakeholders en de toezichthouders.

Robuustheid & wendbaarheid:

- Het streven is om IT-inrichting zo eenvoudig mogelijk te houden met als doel de kwaliteit hoog en de kosten laag te houden. Het bestuur realiseert zich daarbij dat ze daar zelf een belangrijke rol in kan spelen door bijvoorbeeld de regelingen zo eenvoudig mogelijk te houden.
- Het bestuur kiest ervoor om communicatie en uitvoering richting deelnemers te digitaliseren. Het fonds streeft met digitalisering naar een verbetering van de kwaliteit en snelheid als ook een reductie van kosten, waarbij het de intentie is dat het fonds de marktstandaarden volgt. Daarnaast moet IT ook een bijdrage aan de vernieuwing en verbetering van de dienstverlening aan deelnemers leveren.
- IT maakt het mogelijk om innovaties in de pensioenmarkt snel te adopteren. Het moet bijvoorbeeld mogelijk zijn om vereiste wijzigingen in wet- of regelgeving zeer snel en tegen lage kosten door te voeren.
- Het bestuur kiest ervoor om alle processen volgens het principe van straight through processing (STP) in te richten. Dit betekent dat de processen zonder tussenkomst van menselijk handelen worden uitgevoerd. Alleen voor processen waarbij dat onmogelijk of onwenselijk is, wordt dit in beginsel niet gedaan. Dit houdt concreet in dat er in de IT-systemen bij voorkeur een (directe) koppeling dient te bestaan met authentieke bronnen, zoals de Basis Registratie Persoonsgegevens.
- End User Computing (EUC): aansluitend op het principe van STP wordt het gebruik van EUC tot een minimum teruggebracht en alleen toegepast als het niet anders kan. Indien EUC toch wordt toegepast, worden adequate beheersingsmaatregelen ingericht om te borgen dat de doelstellingen van het informatiebeveiligingsbeleid toch gerealiseerd worden.
- Bij IT-investeringsbeslissingen wordt de balans gezocht tussen niveau van gewenste dienstverlening en de daarbij behorende kosten

Betrouwbaarheid

- Het bestuur wenst dat informatieverstrekking aan deelnemers en werkgevers; de verwerking van hun gegevens; en de informatieverstrekking aan het bestuur door uitvoerders juist, tijdig en volledig gebeurt.

Beveiliging & continuïteit

Het bestuur verwacht van uitbestedingspartijen dat zij beleid en processen, waaronder passende strategieën, beleidslijnen, procedures en ICT-protocollen hebben ingericht inzake:

- Het hosten van data in de Europese Unie in geval van cloud-toepassingen met betrekking tot pensioenuitvoering.
- Het goed waarborgen van cybersecurity.
- Het goed waarborgen van business continuity.
- Inzicht in mogelijke key person risks.
- Het doelmatig en rechtvaardig gebruik van persoonsgegevens.

Dit houdt in dat alle informatie- en ICT-activa, met inbegrip van computersoftware, hardware, servers naar behoren en toereikend beschermd moeten worden evenals alle relevante fysieke elementen en infrastructuur, zoals gebouwen en terreinen, datacentra en als gevoelig aangewezen gebieden, om ervoor te zorgen dat alle informatie- en ICT-activa toereikend worden beschermd tegen risico's zoals schade, ongeoorloofde toegang en ongeoorloofd gebruik.

3.4 Risicohouding en risicobereidheidsprincipes

Het bestuur heeft de risicohouding voor het fonds vastgesteld voor (niet-)financiële fondsonderwerpen zoals getoond in onderstaande tabel.

Onderdeel	Risicohouding
Financiële fondsonderwerpen (balansmanagement)	3 (Gebalanceerd)
Niet-financiële onderwerpen (pensioenuitvoering, communicatie, IT en informatiebeveiliging, reputatie, integriteit, compliance, governance)	2 (Kritisch)
BPF Beton in zijn geheel	3 (Gebalanceerd)

De risicohouding voor niet-financiële onderwerpen, zoals IT en informatiebeveiliging is Kritisch (2). Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's relatief laag te houden, vanuit de visie dat gewenste rewards vereisen dat een relatief laag niveau van blootstelling aan risico's wordt geaccepteerd. Idealiter loopt BPF Beton in het geheel geen risico op niet-financiële risico's maar dit is in de praktijk niet haalbaar en weegt ook niet op tegen de gevraagde extra (kosten)inspanningen.

De risicohouding is afgeleid van onderstaande tabel.

Norm	Beschrijving
Nul (1)	Deze risicohouding is gekenmerkt door de wens dat er geen risico's worden genomen, vanuit de visie dat gewenste rewards niet vereisen dat een minimaal niveau van blootstelling aan risico's wordt geaccepteerd.
Kritisch (2)	Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's relatief laag te houden, vanuit de visie dat gewenste rewards vereisen dat een relatief laag niveau van blootstelling aan risico's wordt geaccepteerd.
Gebalanceerd (3)	Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's te balanceren, vanuit de visie dat gewenste rewards vereisen dat een gebalanceerd niveau van blootstelling aan risico's wordt geaccepteerd.
Opportuun (4)	Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's relatief hoog te houden, vanuit de visie dat gewenste rewards vereisen dat een relatief hoog niveau van blootstelling aan risico's wordt geaccepteerd.
Gemaximeerd (5)	De risicohouding is gekenmerkt door de wens dat de blootstelling aan risico's maximaal is, vanuit de visie dat de gewenste rewards vereisen dat een maximale blootstelling aan risico's wordt geaccepteerd.

Voor de beoordeling van beleidsvoorstellen en -uitvoering heeft het bestuur voor informatiebeveiliging de risicobereidheidsprincipes gedefinieerd. Per risicobereidheidsprincipe is

aangegeven op welke wijze kan worden aangetoond dat aan het risicobereidheidsprincipe wordt voldaan (risk appetite indicator) en is de risicotolerantie aangegeven door middel van een streefwaarde inclusief een grens ondermaats en bovenmaats.

Het fonds heeft onderscheid gemaakt naar risicobereidheidsprincipes op strategisch resp. op operationeel niveau.

Strategisch niveau					
Nr.	Risicobereidheidsprincipe	Risk appetite indicator	Streefwaarde	Ondermaats	Bovenmaats
1	Bestuur maakt gebruik van bewezen technologie, volgt de marktontwikkelingen en heeft niet de ambitie om daarin direct voor op te willen lopen	Jaarlijkse beoordeling en evaluatie	1	0	2
2	Wij willen dat pensioenuitvoerder innovatief is en een duidelijke roadmap heeft als het gaat om automatisering met een passend budget	Bespreken en evalueren met uitvoerder	1	0	2
3	IT moet zo ingericht dat noodzakelijke en/of gewenste aanpassingen met een korte doorlooptijd en tegen aanvaardbare kosten te realiseren zijn (wendbaarheid IT)	Jaarlijkse beoordeling en evaluatie	1	0	2
4	Het bestuur verlangt van de uitvoerder dat de informatiebeveiliging en borging data is ingericht en wordt uitgevoerd conform de laatste van wet- en regelgeving en technische mogelijkheden	Jaarlijkse beoordeling en evaluatie	1	0	2
Operationeel niveau					
Nr.	Risicobereidheidsprincipe	Risk appetite indicator	Streefwaarde	Ondermaats	Bovenmaats
1	Gegevensverwerking moet tijdig en volledig zijn, evenals communicatie naar de klant.	aantal werkdagen vertraging	0	5	0
2	Wij willen besluiten nemen op basis van meest actuele, betrouwbare, volledige data, tijdig aangeleverd door uitbestedingsrelaties/adviseurs.	aantal werkdagen vertraging	0	5	0

3	Wij willen business continuity waarborgen zodat onze uitkeringen en premieheffingen tijdig en juist zijn	Recovery time (uren)	24	36	0
4	Wij willen zicht hebben op key person risks (in onderuitbesteding) bij onze uitbestedingsrelaties	Risicoanalyse uitvoeren (per aantal jaren)	1	2	0,5

Dora: duidelijke informatiebeveiligingsdoelstellingen vast te stellen, met inbegrip van kernprestatie-indicatoren en kernrisicomaatstaven; wellicht zijn er door Appel meer KPI's die kunnen worden gevolgd.

3.5 Uitbesteding

BPF Beton is eindverantwoordelijk voor het beheer van ICT-risico's ook als deze risico's in eerste instantie bij de uitbestedingspartijen liggen. Het fonds monitort daarom de uitbestedingspartijen. Daarbij wordt het evenredigheidsbeginsel toegepast, rekening houdend met de aard, de schaal, de complexiteit en het belang van ICT-gerelateerde afhankelijkheden, en de risico's die bij de uitbestede diensten kunnen optreden en het kritieke karakter of het belang van deze diensten, processen of functies en met de potentiële gevolgen voor de continuïteit en de beschikbaarheid van financiële diensten en activiteiten.

Het fonds houdt een informatieregister bij met alle contractuele overeenkomsten over het gebruik van door derde aanbieders verleende ICT-diensten.

Vóór het sluiten van een contractuele overeenkomst inzake het gebruik van ICT-diensten beoordeelt het fonds of deze een kritieke of belangrijke functie ondersteunen en voldoen aan de toezichtvoorwaarden. Alle relevante risico's worden beoordeeld inclusief het concentratierisico. Het fonds verricht een due-diligenceonderzoek over toekomstige derde aanbieders van ICT-diensten en waarborgt gedurende de gehele selectie- en beoordelingsprocedure dat de derde aanbieder van ICT-diensten geschikt is. Het fonds beoordeelt of er belangenconflicten uit de overeenkomsten kunnen voortkomen.

Er worden alleen overeenkomsten gesloten met derde aanbieders van ICT-diensten die voldoen aan passende normen op het gebied van informatiebeveiliging. Wanneer die contractuele overeenkomsten kritieke of belangrijke functies betreffen, dienen zij gebruik te maken van de meest actuele en hoogste normen voor informatiebeveiliging.

Het fonds oefent toegangs-, inspectie- en auditrechten uit ten aanzien van de derde aanbieder van ICT-diensten. Daarvoor wordt vooraf op basis van een risicogebaseerde benadering de frequentie en de te controleren gebieden bepaald. In geval van een grote technische complexiteit, verifieert het fonds of de auditor(s), over passende vaardigheden en kennis beschikken om de desbetreffende audits en beoordelingen doeltreffend uit te voeren.

Het fonds zorgt ervoor een overeenkomst inzake het gebruik van ICT-diensten in elk van de volgende omstandigheden kunnen worden beëindigd:

- bij ernstige overtreding van de toepasselijke wetten, voorschriften of contractuele voorwaarden door de derde aanbieder van ICT-diensten;
- in omstandigheden die in de loop van de monitoring van het ICT-risico van derde aanbieders worden vastgesteld, waarvan wordt aangenomen dat deze wijzigingen kunnen brengen in de uitvoering van de functies waarin de contractuele overeenkomst voorziet, met inbegrip van

materiële wijzigingen die de overeenkomst of de situatie van de derde aanbieder van ICT-diensten nadelig beïnvloeden;

- bij klaarblijkelijke zwakheden van de derde aanbieder van ICT-diensten in verband met zijn algemeen beheer van het ICT-risico en in het bijzonder met de manier waarop hij zorgt voor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van persoonlijke of anderszins gevoelige gegevens of niet-persoonsgebonden gegevens;
- indien de toezichthouder niet langer doeltreffend toezicht kan uitoefenen op het fonds ten gevolge van de voorwaarden van of de omstandigheden in verband met de respectieve contractuele overeenkomst.

Het fonds stelt exitstrategiën op voor ICT-diensten die kritieke of belangrijke functies ondersteunen, waarin rekening wordt gehouden met risico's die zich op het niveau van derde aanbieders van ICT-diensten kunnen voordoen, met name een mogelijk falen van deze aanbieders, een verslechtering van de kwaliteit van de geleverde ICT-diensten, verstoring van de bedrijfsactiviteiten ten gevolge van ongeschikte of falende dienstverlening van ICT-diensten of materiële risico's in verband met de passende en permanente inzet van de respectieve ICT-dienst, of de beëindiging van contractuele overeenkomsten met derde aanbieders van ICT-diensten. Het fonds zorgt er daarbij voor de mogelijkheid te hebben om contractuele overeenkomsten te beëindigen zonder verstoring van de bedrijfsactiviteiten, zonder dat de naleving van de regelgevingsvereisten wordt beperkt en zonder dat afbreuk wordt gedaan aan de continuïteit en de kwaliteit van de diensten van het fonds.

De exitplannen zijn alomvattend en gedocumenteerd en worden voldoende getest en regelmatig geëvalueerd. Het fonds zorgt voor alternatieve oplossingen en ontwikkelt overgangsplannen om in staat te zijn ICT-diensten en de desbetreffende gegevens van de derde aanbieder van ICT-diensten te verwijderen en deze veilig en integraal over te dragen aan alternatieve aanbieders of deze in het fonds zelf te integreren. Het fonds stelt noodmaatregelen op om de bedrijfscontinuïteit te handhaven in geval een exitplan wordt uitgevoerd.

Het fonds let erop te voorkomen dat het een contract sluiten met een derde aanbieder van ICT-diensten die niet gemakkelijk substitueerbaar is, of er een concentratierisico optreedt. Het weegt de baten en kosten af van alternatieve oplossingen, zoals het gebruik van verschillende derde aanbieders van ICT-diensten, rekening houdend met de vraag of en hoe de voorgenomen oplossingen aansluiten bij de zakelijke behoeften en doelstellingen waarin hun strategie inzake digitale weerbaarheid voorziet.

Als kritieke of belangrijke ICT-diensten verder worden uitbesteed, weegt het fonds de baten en risico's hiervan af, met name in het geval van een in een derde land gevestigde ICT-subcontractant. Bij kritieke of belangrijke ICT-diensten houdt het fonds terdege rekening met de faillissementsrisico's van de derde aanbieder. Is de derde aanbieder in een ander land gevestigd, dan houdt het fonds rekening met de naleving van de voor het fonds toepasselijke gegevensbeschermingsregels en de doeltreffende handhaving daarvan in dat land.
Het fonds voorkomt lange of complexe uitbestedingsketens die de monitoring van de dienst voorkomen of de toezichthouder in het toezicht hinderen.

De rechten en plichten van het fonds en de derde aanbieder van ICT-diensten worden duidelijk toegewezen en schriftelijk vastgesteld. Het volledige contract omvat de overeenkomsten inzake dienstverleningsniveau en wordt opgenomen in één schriftelijk document.
De contractuele overeenkomsten inzake het gebruik van ICT-diensten bevatten ten minste de elementen die genoemd worden in DORA artikel 30.2 en 30.3. Zo mogelijk worden de contracten opgesteld aan de hand van modelcontractbepalingen die door overheidsinstanties zijn ontwikkeld voor specifieke diensten.

4. Uitvoering van ICT-risicobeheer

De belangrijkste ICT-systemen voor BPF Beton zijn in beheer van en worden gebruikt door de uitbestedingsrelaties van het fonds. Het risicobeheer van BPF Beton bestaat in die gevallen uit het toezicht op de uitvoering van het risicobeheer op deze systemen door de uitbestedingsrelaties. Het toezicht op het risicobeheer ten aanzien van de pensioenuitvoering kan worden uitgevoerd door controle op de naleving daarvan door de pensioenuitvoeringsorganisatie (Appel Pensioenuitvoering) aan de hand van haar rapportages dienaangaande. De andere uitbestedingsrelaties voor wie het ICT-risicobeheer van belang is voor BPF Beton – met name de custodian en de vermogensbeheerders – zijn geen ICT-dienstverleners maar zijn zelf wel DORA-plichtig. De fiduciair beheerder CTI rapporteert ieder kwartaal over de beoordeling van DORA-vereisten.

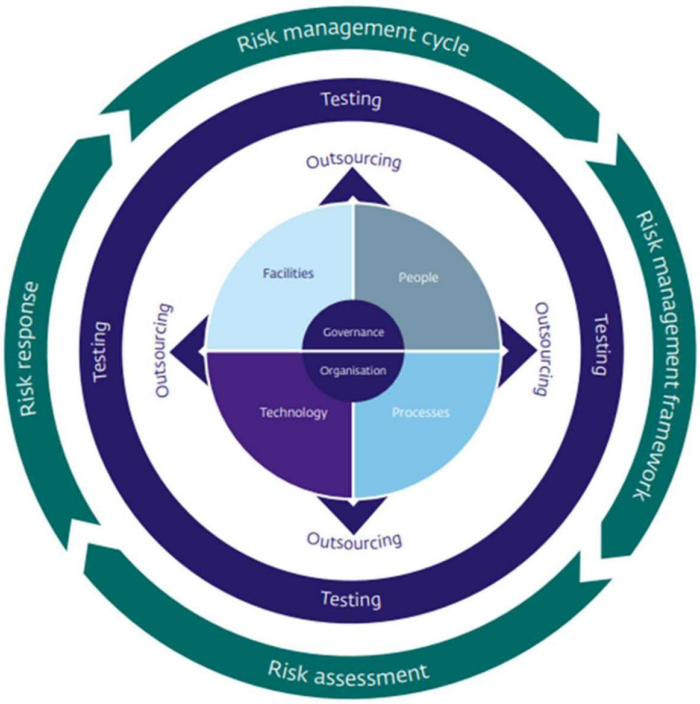
De uitbestedingsrelaties leggen jaarlijks verantwoording af over het geheel van interne beheersmaatregelen door een verklaring van zijn externe accountant middels een ISAE 3402/3000 verklaring, vergelijkbare verklaring en/of Third Party Memorandum (TPM) en rapportages niet-financiële risico's. Op verzoek van het fonds worden gesprekken aangevraagd waarin specifieke thema's inhoudelijk nader worden behandeld.

BPF Beton stelt als voorwaarde dat de uitbestedingsrelatie periodiek audits uitvoeren op de opzet, werking, bestaan van de beheersmaatregelen van informatiebeveiliging in relatie tot de risico's. Bevindingen van deze audits worden met het bestuur van BPF Beton besproken. Ook op initiatief van BPF Beton en/of de sleutelfunctiehouder interne audit kunnen audits worden uitgevoerd.

BPF Beton controleert aan de hand van de rapportages van de uitbestedingsrelaties of de uitbestedingsrelaties (in voldoende mate) aan de bepalingen van de artikelen 9 tot en met 14 van DORA voldoen. Hoofdstuk 3 van DORA (met de voor het fonds relevante artikelen 9 tot en met 14) behandelt de uitvoering van het risicobeheer. In bijlage 3 is opgenomen welke bepalingen dit betreft.

4.1 Uitwerking beleid

Het bestuur heeft het beleid uitgewerkt aan de hand van de acht onderdelen van het DNB Toetsingskader Informatiebeveiliging 2023 zoals weergegeven in onderstaande figuur en aangevuld met de extra vereisten vanuit DORA. De 'Risk Management Cycle' is het proces dat ervoor zorgt dat de opzet, bestaan en werking van de acht onderdelen worden gemonitord door het bestuur. De acht onderdelen zijn ieder verder opgedeeld naar in totaal 58 controls. Het totaaloverzicht van de onderdelen en de controls per onderdeel is opgenomen in bijlage 2.



4.2 Wet en regelgeving, standaarden en best practices

BPF Beton verlangt van haar uitbestedingsrelaties dat zij voor de aanpak en implementatie van maatregelen op het gebied van informatiebeveiliging zich houden aan relevante wet- en regelgeving. Dit betreft onder andere:

- Pensioenwet
    - artikel 143, eerste lid; waarborgen beheerste en integere bedrijfsvoering
- Algemene Verordening Gegevensbescherming (AVG);
- Archiefwet;
- Wet verplichte deelneming in een bedrijfstakpensioenfonds 2000 (Wbpf);
- Sanctiewet (1997)
- Code Pensioenfondsen.
- Guidance uitbesteding door pensioenfondsen, uitgave van de Nederlandsche Bank N.V. van juni 2014.
- DORA.

Daarnaast dient rekening te worden gehouden met geaccepteerde standaarden en best practices.

De uitbestedingsrelaties dienen geschikte, geactualiseerde ICT-systemen, -protocollen en -instrumenten te gebruiken te onderhouden om ICT-risico aan te pakken en te beheren. Deze dienen

- geschikt te zijn voor de omvang van de verrichtingen ter ondersteuning van hun activiteiten
- betrouwbaar te zijn;
- voldoende capaciteit te hebben voor een nauwkeurige verwerking van de gegevens die nodig zijn voor de uitvoering van activiteiten en de tijdige verlening van diensten, en om zo nodig volumepieken in orders, orderberichten of transacties op te vangen, onder meer wanneer nieuwe technologie wordt ingevoerd;
- technologisch gezien voldoende weerbaar te zijn om indien nodig in gespannen marktomstandigheden of andere ongunstige situaties naar behoren te voorzien in bijkomende gegevensverwerking.

4.3 Identificatie, classificatie en documentatie

De daadwerkelijke uitvoering van het risicobeheer begint bij het identificeren van de functies, taken en verantwoordelijkheden die door ICT ondersteund worden. Vervolgens wordt afgeleid waaruit de ICT-risico's bestaan. Voor BPF Beton liggen de belangrijkste functies, taken en (primaire) verantwoordelijkheden bij de uitbestedingspartijen. Dat zijn:

- de pensioenuitvoeringsorganisatie; de belangrijkste ICT- risico's zijn gelegen in de administratie van de pensioenaanspraken en -uitkeringen en de inning van de pensioenpremies, zowel voor wat betreft beschikbaarheid als integriteit en vertrouwelijkheid;
- De custodian, de fiduciair manager en de vermogensbeheerders; ook bij het beheer van de beleggingen van het fonds spelen ICT-risico's een belangrijke rol. Beschikbaarheid en integriteit zijn hier de belangrijkste aandachtsgebieden.

De risico's worden gedocumenteerd en geclassificeerd volgens de BIV-analyse, zie 4.3.2.

De identificatie en vervolgens documentatie en classificatie is een permanent proces. Ten minste eenmaal per jaar beoordeelt de IRM-commissie of de documentatie en classificatie nog adequaat is. Daarnaast worden risicoscenario's geëvalueerd die zich kunnen voordoen, onder meer vanuit cyberdreigingen en ICT-kwetsbaarheden. Bij belangrijke wijzigingen in de ICT-infrastructuur, -processen of -procedures worden de risico's opnieuw beoordeeld.

De IRM-commissie maakt - voor zover deze informatie door de uitbestedingspartijen wordt gedeeld - een inventarisatie van de (cruciale) informatie- en ICT-activa, netwerkmiddelen en hardware-uitrusting bij de uitbestedingspartners en bij het fonds, de configuratie daarvan en de verbanden en onderlinge afhankelijkheden. In het bijzonder acht de commissie de inventarisatie door Appel van belang. Eerder is die bij de beoordeling van de datakwaliteit langsgekomen.

4.3.1 BIV-analyse

Voor de identificatie van belangrijkste risico's hanteert BPF Beton een rating vanuit de BIV-analyse. Dit is een analyse van de risico's van de belangrijkste systemen van de uitbestedingspartners op de onderdelen Beschikbaarheid, Integriteit en Vertrouwelijkheid. Qua indeling duiden we per categorie met 1, 2, en 3 de zwaarte van het risico aan. Waar '1' staat voor laag en '3' voor hoog risico. Met de uitbestedingspartijen wordt overeengekomen dat zij beheersmaatregelen hebben geïmplementeerd overeenkomstig het beleid van het fonds. Tevens wordt met de uitbestedingspartner per systeem een maximale uitval afgesproken. Hoe hoger het risiconiveau, hoe korter de maximale uitvaltijd. De BIV-classificatie is opgenomen in bijlage 1 van dit document.

4.3.2 Beschikbaarheid

De uitbestedingsrelatie waarborgt dat de geautoriseerde gebruikers op de juiste momenten tijdig toegang verkrijgen tot de informatie van BPF Beton door middel van relevante bedrijfsmiddelen. De uitvoeringssystemen zijn beveiligd en bij uitval geldt een maximale recovery tijd. Daarover spreekt het BPF Beton met de uitbestedingsrelatie de grenzen van recovery af.

4.3.2 Integriteit

De informatie van het BPF Beton dient juist en volledig te zijn. Daartoe zet de uitbestedingsrelatie de relevante bedrijfsmiddelen in en overlegt deze met het bestuur van het pensioenfonds.

4.3.3 Vertrouwelijkheid

Informatie is alleen toegankelijk voor de bevoegde personen. Bestuurders, leden van de Raad van Toezicht en het Verantwoordingsorgaan gaan vertrouwelijk om met informatie. Daarbij maakt het pensioenfonds gebruik van een beveiligd digitaal platform voor alle fondsdocumenten en

vergaderstukken. In voorleggers wordt op anonieme wijze gesproken over belanghebbenden van het pensioenfonds.
Met de uitbestedingsrelatie komt BPF Beton overeen wie als bevoegde personen kunnen worden aangewezen. Functiescheiding wordt toegepast om het botsen van belangen tegen te gaan en de kans op frauduleus handelen te beperken.
Het management van de uitbestedingsrelatie is verantwoordelijk voor het opstellen, inrichten en naleven van het beleid.

4.4 Mensen (People)

Het is belangrijk dat alle medewerkers, externe inhuur en dienstverleners bekend zijn met het informatiebeveiligingsbeleid van BPF Beton, hun verantwoordelijkheden kennen en kunnen (blijven) werken volgens dit beleid en de risicobereidheid van BPF Beton. Het bestuur is eindverantwoordelijk voor het (blijvend) zorgdragen voor een passend kennisniveau van medewerkers en ziet erop toe dat alle elementen van informatiebeveiliging en cybersecurity zijn beheerst.
Goed opdrachtgeverschap: het bestuur ziet erop toe dat de uitbestedingspartijen hun afspraken nakomen ten aanzien van de personele aspecten van informatiebeveiliging en cybersecurity zoals hierboven genoemd.

4.4.1 Bestuur en personeel

Bestuurders, leden van organen van het pensioenfonds en personeel van de uitbestedingsrelaties worden voorafgaand aan het dienstverband geïnformeerd over de verantwoordelijkheden ten aanzien van informatiebeveiliging. Deze verantwoordelijkheden zijn voor bestuurders (verbonden personen) vastgelegd in de gedragscode van het pensioenfonds. De gedragscode is op de site van BPF Beton beschikbaar. Voor personeel van de uitbestedingsrelatie geldt dat zij middels de (arbeids)overeenkomst en functiebeschrijvingen worden geïnformeerd.
Voorafgaand aan het lidmaatschap binnen het bestuur vindt een screening plaats. Dat geschiedt via de gemeente door een Verklaring Omtrent het Gedrag op te vragen. Nadere omschrijving van de screening is beschikbaar in het screeningsbeleid.
De uitbestedingsrelatie wordt geacht voorafgaand aan een dienstverband van haar medewerker(s) altijd een Pre Employment Screening (PES) van de medewerker te verzorgen. Verder moeten medewerkers meewerken aan een verzoek tot screening en/of het verstrekken van een Verklaring Omtrent het Gedrag (VOG).
Tijdens en na beëindiging van het bestuurslidmaatschap dan wel de (arbeids)overeenkomst van de werknemers van uitbestedingsrelaties, zijn bestuurders, medewerkers, ingehuurd personeel en externe gebruikers verplicht tot geheimhouding van alle informatie en/of kennis die hij/zij heeft gekregen over BPF Beton, de eigen organisatie, gelieerde ondernemingen en opdrachtgevers van de organisatie.

4.4.2 Bewustzijn, opleiding en training

Bestuurders en andere verbonden personen verklaren door het ondertekenen van de gedragscode dat zij zich bewust zijn van het infomatiebeveiligingsbeleid en de afspraken ten aanzien van vertrouwelijkheid en geheimhouding.
BPF Beton controleert of de uitbestedingsrelaties voor hun personeel een passend bewustzijns-, opleidings- en trainingsbeleid heeft (zie bijlage 3, DORA artikel 13.6 en 13.7).

4.4.3 Sancties

Indien het bestuur constateert dat een verbonden persoon zich niet houdt aan de gestelde richtlijnen van informatiebeveiliging, gaat het in gesprek met betreffende persoon. Alleen als blijkt dat het om een bewust ongeoorloofd handelen gaat zal het bestuur passende maatregelen treffen. Sancties met betrekking tot ongeoorloofd handelen bij de uitbestedingsrelatie dienen aldaar te zijn vastgelegd en uitgevoerd.

4.4.4 Beëindiging bestuurderschap of het dienstverband

Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging van het bestuurder lidmaatschap zijn verankerd in de gedragscode. De uitbestedingsrelatie communiceert aan zijn werknemer(s) bij beëindiging van het dienstverband welke verantwoordelijkheden ook na het eindigen van de arbeidsovereenkomst van kracht blijven. Tevens worden toegangsrechten en user-id's verwijderd, en bedrijfsmiddelen ingeleverd.

4.5 Processen

Het bestuur is eindverantwoordelijk voor het zorgdragen en/of controleren dat de strategie en het overall IT-security plan in lijn is met de richtlijnen van het bestuur en de overige bedrijfsprocedures met betrekking tot:

- Continuïteit van de operatie.
- Het beheersen van incidenten inclusief beleid inzake escalatie.
- Het op beheerste wijze wijzigingen doorvoeren zonder verstoring van het informatiebeveiligingsniveau en/of de data-integriteit negatief beïnvloeden.
- Het uitvoeren van de testprocedures afgescheiden van de productieomgeving.
- De kwaliteit van de IT-beheerprocessen.

4.5.1 Melden van (beveiligings)incidenten

Informatiebeveiligingsincidenten en eventuele geconstateerde zwakke plekken in de beveiliging, worden door het bestuur van het pensioenfonds direct besproken en verholpen. Wijzigingen in het informatiebeveiligingsbeleid worden met de verbonden personen en uitbestedingsrelaties binnen twee weken na vaststelling gecommuniceerd. Zwaarwegende incidenten worden aan DNB gemeld.

De specifieke eisen aan het melden van incidenten (door Appel) zijn nog in voorbereiding: beoogd wordt dat Appel binnen 4 uur de eerste melding dient te activeren. Voorafgaand aan de tweede melding vindt overleg met het fonds plaats. Terugkoppeling verwacht de IRM-commissie vanuit het SFHO Appel en dat voorstel wordt aan het bestuur voorgelegd. Incidenten dan wel constatering van zwakke plekken bij de uitbestedingsrelatie en haar (eventuele (toe)leveranciers behoren onverwijld te worden gerapporteerd aan BPF Beton en toegelicht. Van de incidenten op het vlak van informatiebeveiliging wordt door de uitbestedingsrelatie een incidentenregister bijgehouden. Het samenstel hiervan vormt het incidentenregister van BPF Beton. In het incidentenregister wordt het incident beschreven, de effecten ervan, de wijze waarop het incident is bestreden en de doeltreffendheid daarvan. Indien van toepassing worden de preventiemaatregelen genoemd die soortgelijke incidenten in de toekomst kunnen helpen voorkomen.

Het fonds houdt het aantal gemelde ernstige incidenten bij en de doeltreffendheid van de maatregelen. Hiermee kan het fonds een beeld verkrijgen en tonen van de actuele status van de digitale operationele weerbaarheid.

4.5.2 Bedrijfsmiddelen

Voor de werknemer van een uitbestedingsrelatie geldt dat (bedrijfs)middelen die toegang en/of autorisatie faciliteren tot informatie en deze kunnen opslaan, ondersteunen en/of essentieel zijn binnen de bedrijfsvoering, worden geregistreerd en gekoppeld aan een eigenaar. De uitbestedingsrelatie is verantwoordelijk voor de juiste classificatie en de toegepaste beveiligingsmaatregelen.

4.5.3 Opslag van informatie

Het BPF Beton slaat informatie zoveel mogelijk digitaal op. Opslag vindt plaats via OurMeeting, een beveiligde omgeving waar een strikte autorisatiescheiding is toegepast. Verbonden personen krijgen alleen toegang tot de voor hen relevante informatie. In het privacyreglement staat

beschreven op welke wijze het pensioenfonds omgaat met (persoons)gegevens en hoe lang deze worden bewaard. De fondsspecifieke informatie wordt door de dienst “bestuursondersteuning” op een alleen voor hen toegankelijke schijf opgeslagen. De pensioenuitvoeringsorganisatie faciliteert en bewaakt dit proces. De uitbestedingsrelatie draagt er zorg voor dat informatie(dragers) worden bewaard op een locatie met beveiligingsmaatregelen die in overeenstemming zijn met de classificatie van de betreffende informatie.

4.5.4 Printen van informatie

Bij het printen van informatie zijn de verbonden personen gehouden zorgvuldig om te gaan met de output. Indien het fysieke stuk niet langer hoeft te worden bewaard, wordt de print vernietigd. Vanwege de gevoelige klantinformatie die beschikbaar is bij de uitbestedingsrelatie(s), past de uitbestedingsrelatie een beveiligd printsysteem toe.

4.5.5 Verstrekken van informatie

De uitbestedingsrelatie verstrekt (deelnemer) informatie bij voorkeur via de standaard digitale of schriftelijke kanalen. Het telefonisch verstrekken van deze informatie is pas toegestaan wanneer vaststaat dat het de deelnemer of een gemachtigde derde betreft. Dan wel een aan de uitbestedingsrelatie verbonden persoon. Er bestaat een protocol waarmee de identiteit van de informatievrager wordt vastgesteld.

4.5.6 Verstrekken van fondsinformatie

Het verstrekken van fondsinformatie aan derden (bijvoorbeeld DNB, AFM), voor zover dit niet wettelijk verplicht is, vindt pas plaats na schriftelijk akkoord van het fonds.

4.5.7 Verwijderen en vernietigen van informatie

Verwijderen en vernietigen van informatie vindt gecontroleerd plaats conform de afspraken tussen het pensioenfonds en de uitbestedingsrelatie. Daarbij gelden de volgende uitgangspunten:

Onderwerp	V1 Openbaar	V2 Intern gebruik	V3 Vertrouwelijk
Verwijderen digitale media	Vrij	Delete; Bij levering media aan derden: via speciale tooling	Afvoeren en vernietigen door een gespecialiseerde organisatie onder overhandiging van certificaat. Voor het verwijderen van fonds en klantinformatie bestaat een protocol.
Verwijderen papieren documenten	Vrij	Papierbak/afgesloten container.	Afgesloten container/shredder

4.5.8 Bewaartermijnen

Fonds- en deelnemerinformatie wordt bewaard zoals beschreven in het privacyreglement en zoals afgesproken in de contracten met uitbestedingsrelaties. Voor het verwijderen en vernietigen van informatie in geval van einde bewaartermijn hanteert de uitbestedingsrelatie een vaste procedure in lijn met het privacyreglement van BPF Beton.

4.5.9 Wijzigingsbeheer

Het up-to-date houden van programmatuur is van groot belang om kwetsbaarheden te beperken. Hierdoor is het noodzakelijk dat o.a. notebooks periodiek de updates kunnen installeren. Updates worden vaak automatisch uitgevoerd.

4.5.10 Scheiding Ontwikkel-Test-Productie-omgevingen

Om te zorgen dat databases van de uitbestedingsrelatie niet bevuild raken met testgegevens en/of productiegegevens onbedoeld in een testomgeving terecht komen, is het van belang dat in elke fase van software ontwikkeling goed overwogen wordt welke (test)gegevens nodig zijn en hoe deze gegevens eruit zien. Er worden geen productiegegevens van BPF Beton gebruikt, gegevens worden (zoveel mogelijk) geanonimiseerd en het aantal aangeleverde velden zo beperkt mogelijk gehouden.
Voor verzending van deze geanonimiseerde testbestanden wordt gebruik gemaakt van een wijze van versleuteling. Afspraak hierbij is dat separaat een wachtwoord wordt verstuurd via een niet publiekelijk toegankelijk kanaal (bijv. mondeling/sms).

4.5.11 Leveranciersrelaties

Uitbestedingsrelaties doen zaken met (vele) leveranciers. Het is van groot belang dat deze leveranciers voortdurend passende maatregelen nemen om de informatie te beveiligen en de continuïteit van de onderneming te waarborgen. Daar waar van toepassing hanteert de uitbestedingsrelatie ten aanzien van de specifieke informatiebeveiligingsaspecten de volgende uitgangspunten:

- Indien de uitbestedingsrelatie gebruik maakt van (toe)leveranciers dan gelden voor hen minimaal dezelfde (informatiebeveiligings)eisen als het BPF Beton stelt voor de uitbestedingsrelatie.
- De uitbestedingsrelatie neemt alleen producten en/ of diensten van (toe)leveranciers af die voldoen aan de gestelde beveiligingseisen van BPF Beton voor dat product of die dienst.
- De uitbestedingsrelatie documenteert de (toe)leveranciers en rapporteert daarover aan het bestuur van BPF Beton.

Daar waar van toepassing worden in alle leverancierscontracten en bijhorende SLA afspraken de relevante afspraken en rechten en plichten van beide partijen op het gebied van informatiebeveiliging opgenomen (informatiebeveiligingsparagraaf).
Uitgangspunten binnen de betreffende informatiebeveiligingsparagraaf zijn:

- Dienstverlening van Leverancier is compliant aan geldende wet- en regelgeving;
- Leverancier conformeert zich aan het Informatiebeveiligingsbeleid van BPF Beton;
- Het beveiligingsniveau binnen de dienstverlening door Leverancier voldoet minimaal aan het geldende (basis)niveau van beveiliging van BPF Beton;
- Leverancier geeft zekerheden ten aanzien van het overeengekomen niveau van informatiebeveiliging (bijvoorbeeld certificaat, derden verklaring);
- De uitbestedingsrelatie heeft het recht om de informatiebeveiliging binnen de dienstverlening met (toe)leveranciers periodiek te beoordelen (audit);
- Er worden afspraken gemaakt over incidentafhandeling, communicatie en het informeren van het bestuur van BPF Beton in geval van een incident en/of datalek bij de (toe)leverancier.

4.5.12 Continuïteit management

De continuïteit van de bedrijfsvoering van de uitbestedingsrelatie is van significant belang. De uitbestedingsrelatie neemt maatregelen om de continuïteit te waarborgen en rapporteert daarover tijdens de jaarlijkse evaluatie.

4.5.13 Business Impact Analyse

De uitbestedingsrelatie stelt de gewenste minimale mate van beschikbaarheid jaarlijks, en in ieder

geval bij relevante wijzigingen, vast door middel van een Business Impact Analyse (BIA). Binnen deze BIA wordt een kwalitatieve inschaling van de verwachte impact vastgesteld van een gebeurtenis die leidt tot het niet beschikbaar zijn van de betreffende informatie(voorziening) gedurende een bepaalde tijd. Ook wordt binnen de BIA de maximaal acceptabele mate van dataverlies bepaald. De BIA dient te worden uitgevoerd in de gevallen waarbij de keuze voor / selectie van continuïteit verhogende maatregelen (bijv. dubbel uitvoeren systemen, uitwijkregeling, eisen aan leveranciers) voorligt.

4.5.14 Business Continuity Plan

De uitbestedingsrelatie stelt een Business Continuity Plan (BCP) op, gericht op het adequaat omgaan met gebeurtenissen die de beschikbaarheid van de informatievoorziening op centraal bedrijfsniveau raakt. Binnen dit plan is een continuïteitsorganisatie gedefinieerd, waarbinnen een Crisis Management Team (CMT) een centrale positie inneemt.
De uitbestedingsrelatie stelt voor zichzelf en voor de bedrijfsprocessen en (IT-)bedrijfsmiddelen van derden in beheer, een continuïteitsplan op inclusief een uitwijkplan.

4.5.15 Uitwijkvoorziening

De uitbestedingsrelatie maakt gebruik van een beveiligde uitwijkvoorziening zoals bijvoorbeeld een “Twin Data Center”. De beveiliging geschiedt conform de normen en richtlijnen voor de afzonderlijk behandelde onderdelen in dit Informatiebeveiligingsbeleid. Voor zover hierbij gebruik wordt gemaakt van de diensten van derden worden hiervoor Third Party Memorandums (TPM’s) opgesteld.

4.5.16 Back-up en recovery

De uitbestedingsrelatie maakt dagelijks back-ups van gegevens en programmatuur om bij verstoringen de gegevens te kunnen herstellen. Periodiek (minimaal jaarlijks) wordt een back up and recovery test uitgevoerd.

4.6 Technologie

4.6.1 Autorisatie

Ten aanzien van autorisaties gelden de volgende voorwaarden:

- een gebruiker (medewerker van de uitbestedingsrelatie) wordt geïdentificeerd met een unieke user-id;
- user-id’s en wachtwoorden zijn persoonsgebonden en niet overdraagbaar;
- user-id’s en wachtwoorden mogen niet worden gedeeld;

Het management van de uitbestedingsrelatie is verantwoordelijk voor het toekennen van autorisaties.

4.6.2 Wachtwoorden

Wachtwoorden dienen minimaal te voldoen aan de volgende kenmerken:

- minimale lengte: 8 karakters;
- gebruik van combinatie van hoofdletters, kleine letters, leestekens, cijfers;
- vermijdt reguliere woorden en/of eenvoudig herleidbare namen;
- wachtwoorden dienen periodiek (minimaal jaarlijks) gewijzigd te worden.

4.6.3 Toegang via (mobiele) devices

Devices (apparatuur) die worden gebruikt om toegang te verkrijgen tot het netwerk van de uitbestedingsrelatie dienen zogenaamde managed devices te zijn. De uitbestedingsrelatie beheert en bewaakt deze devices.

4.6.4 Externe toegang

Het netwerk van de uitbestedingsrelatie mag alleen van buiten betreffende locatie van de relatie

benaderd worden via een versleutelde verbinding en two-factor authenticatie.

4.6.5 Authenticatie

De authenticatie van gebruikers dient minimaal te voldoen aan de ‘two-factor’ standaard. Dit wil zeggen dat de authenticatie minimaal twee van de volgende authenticatiefactoren vereist: Iets wat je weet (bijv. wachtwoord, pincode), iets wat je hebt (bijv. token, pasje, managed device/certificaat), iets wat je ‘bent’ (bijv. vingerafdruk, iris-scan).

4.6.6 High privileged accounts

Het gebruik van accounts met hoge rechten (high privileged accounts), zoals root- en beheerdersaccounts is slechts toegestaan als deze noodzakelijk zijn voor de uitvoering van specifieke beheertaken. Hiervoor dienen de gebruikers van deze accounts een schriftelijk akkoord te hebben van de uitbestedingsrelatie. Na afronding van de werkzaamheden moet het account direct geblokkeerd worden. Elk gebruik van high privileged accounts moet gelogd en gemonitord worden.

4.6.7 Cryptografie

Opslag en transport van informatie door de uitbestedingsrelatie met een bepaalde mate van vertrouwelijkheid (V2 of V3), dient op een versleutelde wijze te gebeuren.

4.6.8 Opslag op digitale media

Wanneer opslag van informatie met classificatie V3 op digitale verwijderbare media plaatsvindt (bijv. externe schijf, usb-device), dient de informatie versleuteld te zijn.

4.6.9 Bestanden

Daar waar dat door wet- en regelgeving wordt gevraagd en/of wanneer dit bijvoorbeeld vanwege de specifieke aard van de informatie wenselijk wordt geacht, worden bestanden die informatie met classificatie V3 bevatten, voorzien van een (sterk)wachtwoord. Het wachtwoord moet op een veilige, separate locatie (dus niet op dezelfde schijf) opgeslagen worden en via een separaat kanaal gecommuniceerd worden.

4.6.10 Databases

Daar waar dat door wet- en regelgeving wordt gevraagd en/of wanneer dit bijvoorbeeld vanwege de specifieke aard van de informatie wenselijk wordt geacht (bijv. in geval van persoonsgegevens), worden databases die informatie met classificatie V3 bevatten, adequaat versleuteld. De sleutel dient separaat en adequaat beheerd te worden.

4.6.11 E-mail

Voor e-mail past het bestuur van BPF Beton een beveiligde omgeving toe. Alle e-mailadressen van de bestuursleden zullen worden gefaciliteerd via een speciaal beveiligde omgeving vanuit de pensioenuitvoeringsorganisatie. De uitvoeringsorganisatie werkt aan de inrichting van het beoogde mailverkeer.
Informatie met classificatie V3 wordt niet via e-mail verspreid. In die gevallen wanneer verzending noodzakelijk is, wordt gebruik gemaakt van File Transfer of een andere wijze van versleuteling. Afspraak hierbij is dat separaat een wachtwoord wordt verstuurd via een niet publiekelijk toegankelijk kanaal (bijv. mondeling/sms).

4.6.12 Beheersmaatregelen tegen malware

De uitbestedingsrelatie neemt technische maatregelen om malware en virussen ‘buiten de deur’ te houden. De medewerker van de uitbestedingsrelatie wordt geacht er voor te zorgen dat besmetting door/met malware zo veel als mogelijk wordt voorkomen.

4.6.13 Communicatiebeveiliging
Het netwerk van de uitbestedingsrelatie dient met (diverse) technische en organisatorische maatregelen te zijn beveiligd en worden beheerd. Het uitgangspunt hierbij is dat er een zogenaamde gelaagde beveiliging plaatsvindt. Het idee achter deze benadering is dat systemen en informatie wordt beschermd tegen aantasting van de Vertrouwelijkheid, Integriteit en Beschikbaarheid, met behulp van verschillende onafhankelijke methoden en technieken. De betreffende maatregelen variëren in aard.
Zo is er onderscheid te maken in: preventieve, detectieve, correctieve en repressieve maatregelen. Wanneer er binnen de werkzaamheden gebruik kan worden gemaakt van een thuisnetwerkomgeving, dient deze omgeving adequaat beveiligd te zijn. Dat wil zeggen dat deze omgeving minimaal is voorzien van de laatste beveiligingsupdates, firewall-functionaliteit, bescherming tegen malware. Ook is het wenselijk om het standaardwachtwoord van een Wifi-access point te wijzigen.

4.6.14 Het beheer van de netwerkbeveiliging
Het beheer van de netwerkbeveiliging vindt gestructureerd plaats op basis van de principes van procesmatig IT service management . De uitbestedingsrelatie informeert het bestuur op welke wijze het beheer plaatsvindt.

4.6.15 Scheiding in netwerken
Vanuit beveiligingsperspectief is het van belang dat netwerken met een onderling afwijkende gebruiksaard en/of gebruikersdoelgroep (gasten / klanten / beheer / demo / test / productie) logisch dan wel fysiek van elkaar zijn gescheiden.

4.7 Faciliteiten

4.7.1 Clouddiensten
Er gelden restricties ten aanzien van het gebruik van clouddiensten. Het toegestane gebruik van dergelijke diensten gekoppeld aan de classificatie van de informatie. De diensten worden door de uitbestedingsrelatie gehost en beheerd vanuit een datacenter van een service provider die door de uitbestedingsrelatie is aangesteld.

4.7.2 Fysieke beveiliging en beveiliging van de omgeving
Fysieke beveiliging omvat het fysiek afschermen, beschermen en afsluiten van ruimten met geschikte beveiligingsbarrières en toegangsbeveiliging om aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te voorkomen.

4.7.3 Algemene toegang
Ten aanzien van de algemene toegang van bedrijfsruimte en afdelingen wordt als uitgangspunt gehanteerd dat de uitbestedingsrelatie toeziet op autorisatie. Bezoekers melden zich bij de receptie en worden gedurende het bezoek begeleid. Ook krijgen zij een bezoekerspas.

4.8 Uitbesteding
Het fonds heeft het pensioenbeheer en de het vermogensbeheer uitbesteed aan externe partijen omdat het fonds meent dat externe partijen de werkzaamheden van kwalitatief hoog niveau op efficiënte wijze kunnen uitvoeren in vergelijking tot eigen beheer door fonds zelf.
Uitbesteding brengt naast voordelen ook risico's met zich mee op het gebied van informatiebeveiliging en cybersecurity. Onderdeel van het selectieproces is het opstellen van een risico-analyse. Tijdens het uitbestedingsproces wordt afspraken gemaakt over:

- De naleving van het informatiebeveiligingsbeleid van het fonds door de uitbestedingspartij. Uitgangspunt is dat voldaan wordt aan de 58 beheersingsmaatregelen uit de DNB good practice Informatiebeveiliging 2023.

- De wijze waarop de uitbestedingspartij rapporteert over o.a. informatiebeveiliging en beheersing van het cybersecurity risico inclusief eventueel aangestelde subcontractors.
- De uitbestedingspartner stuurt bij op het moment dat risicotoleranties worden overschreden.

Het uitbestedingsbeleid van het fonds is leidend voor de uitvoering van het selectieproces. Het selectieproces wordt uitgevoerd in lijn met de DNB Guidance uitbesteding door pensioenfondsen (juni 2014).

4.9 (Security) Testing

Het bestuur ziet erop toe dat bij de uitbestedingsorganisaties er periodiek security testing plaats vindt op de diverse onderdelen van het model bijvoorbeeld technologie, mensen, faciliteiten. Het fonds kan dat ook zelf uitvoeren – met inzet van voldoende middelen en zonder belangenconflicten - of een derde daartoe opdracht geven. Ook kan het uitgevoerde beheersmaatregelen zoals deze door de uitbestedingspartij onafhankelijk laten testen door een daartoe aangestelde externe partij. Het bestuur ziet erop toe dat de uitbestedingsorganisatie ten minste eenmaal per jaar passende tests uitvoert op alle ICT-systemen en -toepassingen die kritieke of belangrijke functies ondersteunen.

Security testing is bedoeld om het bestuur een onafhankelijk volledig en transparant beeld te verstrekken over de geteste onderdelen met het doel te kunnen beoordelen of de processen voldoende robuust zijn of aanpassing vergen, voor de beoordeling van de paraatheid bij de behandeling van ICT-gerelateerde incidenten, de omschrijving van zwakheden, gebreken en lacunes in de digitale operationele weerbaarheid, en de snelle uitvoering van corrigerende maatregelen.

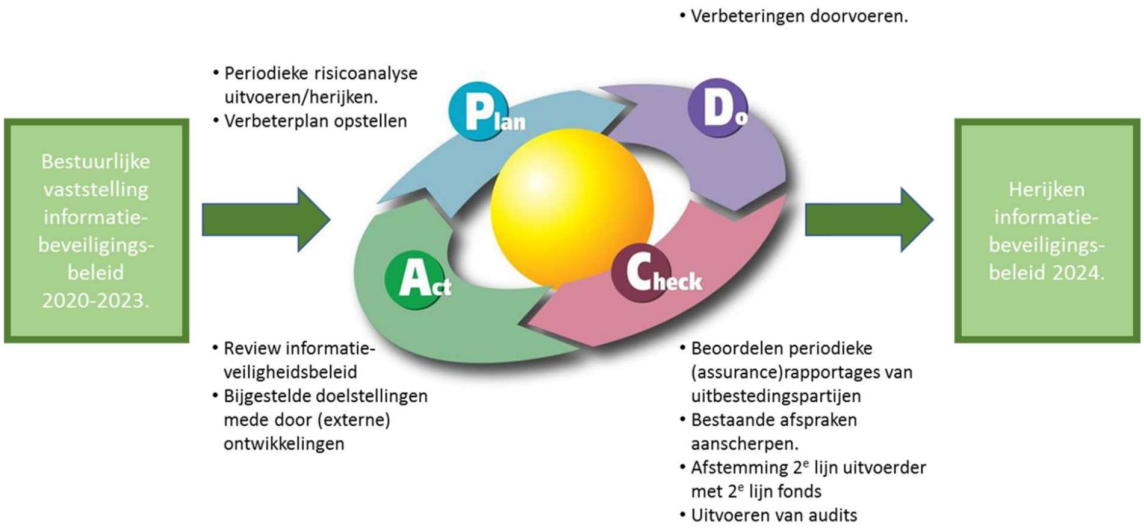
Het testprogramma is risicogebaseerd, waarbij rekening wordt gehouden met het veranderende landschap van het ICT-risico en met specifieke risico's waaraan het fonds wordt of kan worden blootgesteld, de kritieke aard van informatieactiva en verleende diensten. Hierbij moet gedacht worden aan datalekken en incidenten rond de uitbetaling van pensioen en inning van premie.

Het testprogramma kan bestaan uit kwetsbaarheidsbeoordelingen en -scans, opensourceanalyses, netwerkbeveiligingsbeoordelingen, kloofanalyses, beoordelingen van fysieke beveiliging, vragenlijsten en scanningsoftwareoplossingen, beoordelingen van broncodes indien mogelijk, scenariogebaseerde tests, compatibiliteitstests, prestatietests, eind-tot-eindtests en penetratietests.

Het fonds zorgt ervoor dat de uitbestedingsorganisaties alle in de tests gesignaleerde problemen classificeert, prioriteert en verhelpt. Het bestuur monitort de aanpak van de vastgestelde zwakheden, gebreken of lacunes.

4.10 (Risicomanagement) Proces

In de uitvoering van dit beleidsdocument informatieveiligheid maakt het bestuur gebruik van de Plan-Do-Check-Act cyclus zoals onderstaand weergegeven (met als voorbeeld de herijking in 2024).



Plan

Het bestuur is verantwoordelijk voor de uitvoering van dit beleid. De uitvoering van het informatiebeveiligingsbeleid is gedelegeerd aan de IRM-commissie. De IRM-commissie voert regie op de uitvoering van het beleid en stelt hiertoe een jaarkalender op.
De uitkomsten uit de periodieke risicoanalyse kunnen aanleiding geven tot het opstellen van een verbeterplan. Met de uitbestedingspartijen zijn/worden afspraken gemaakt over naleving van het informatiebeveiligingsbeleid. Daarbij streeft BPF Beton ernaar te komen tot een sluitende rapportagelijn tussen het fonds en de uitbestedingspartij. De eisen van het fonds worden in overleg met de uitbestedingspartijen vastgesteld en sluiten aan op het DNB self assessment informatieveiligheid. De belangrijkste eisen zullen vervolgens ook in de SLA met de betreffende uitbestedingspartijen worden opgenomen, inclusief afspraken over de wijze van rapportage. Indien een leverancier niet kan voldoen aan deze eisen, wordt hij uitgesloten.

BPF Beton sluit zich aan bij (internationaal) erkende standaarden op IT-gebied, zoals de 58 controls van het DNB self assessment informatieveiligheid vanaf 2024. Bij uitbesteding toetst BPF Beton, als één van de (potentiële) klanten, of de uitbestedingspartner voldoet aan het IT-beleid van het fonds, de wet- en regelgeving en het DNB IT Toetsingskader. Bij het afsluiten van het contract met de beoogde uitbestedingspartij moet echter duidelijk zijn dat de risico's van BPF Beton worden beheerst. Tegelijkertijd wordt het contract met de uitbestedingspartij beoordeeld op een sluitende rapportagelijn met betrekking tot informatiebeveiliging.
Het fonds moet voldoen aan de controls zoals gedefinieerd in het DNB IT Toetsingskader. Periodiek vraagt het fonds de door de aangestelde uitbestedingspartijen ingevulde DNB IT Toetsingskader op en beoordeelt deze en indien nodig stemt deze nader af met de uitbestedingspartij. Daarnaast wil BPF Beton de specifieke risico's voor de pensioensector in Nederland afdekken, in aanmerking nemend dat BPF Beton geen risico's heeft die nóg specifieker zijn. BPF Beton beschouwt de beheersing van de privacy en het cybersecurity risico als de voornaamste risico's. De kans dat deze risico's zich voordoen zijn het grootst bij de pensioenadministrateur.

Do

De IRM-commissie zorgt voor de uitvoering en waar nodig implementatie van het verbeterplan. De uitkomsten worden gerapporteerd aan het bestuur. Indien besluitvorming van het bestuur nodig is dan legt de IRM-commissie een advies voor aan het bestuur ter bekrachtiging.

Check

De uitbestedingspartners managen de beheersingsmaatregelen in de uitvoeringsfase (Deliver and Support). Het bestuur laat zich hierover informeren via SLA-rapportages, ISAE 3402 rapporten en eventuele andere (niet-financiële) rapportages of relevante certificaten zoals ISO 27001 of 27002. Naast deze standaardrapportages laat het bestuur zich informeren over:

- incidenten en de afhandeling daarvan;
- datalekken en de afhandeling daarvan;
- belangrijke stappen in strategische projecten, afhankelijk van de afspraken terzake.

De belangrijkste activiteiten bestaan uit het beoordelen van de SLA-rapportages, de ISAE-3402-type 2 rapporten en aanvullende rapportages over incidenten en datalekken. De IRM-commissie voorziet het bestuur van haar bevindingen en aanbevelingen bij deze rapportages.

Act

Het beleid wordt voor drie jaar vastgesteld. Evaluatie van het beleid gebeurt jaarlijks en wanneer daartoe aanleiding bestaat. Het herijken van de risicoanalyse kan eveneens nieuwe input leveren om het informatiebeveiligingsbeleid aan te passen.

4.11 Risicobeheersing

4.11.1 ICT-gerelateerde incidenten

De uitbestedingsrelaties houden processen in stand om ICT-gerelateerde incidenten en significante cyberdreigingen te detecteren en registreren, te beheren, behandelen en monitoren en te melden, met als doel de onderliggende oorzaken op te sporen, te documenteren en weg te nemen om dergelijke incidenten te voorkomen. Daarbij zorgen zij voor een categorisatie en classificatie naar prioriteit en ernst en het belang van de getroffen diensten. Cyberdreigingen worden als significant geclassificeerd op basis van de mate waarin de risicovolle diensten, waaronder de transacties en verrichtingen van het fonds, als cruciaal kunnen worden aangemerkt, het aantal en/of de relevantie van de betroffenen of financiële tegenpartijen en de geografische spreiding van de risicogebieden. De pensioenuitvoeringsorganisatie heeft plannen opgesteld voor communicatie met het fonds en de (gewezen) deelnemers, pensioengerechtigden en werkgevers, voor mededeling aan het fonds en voor verstrekking van informatie aan het fonds. Ten minste de ernstige incidenten worden aan het hogere leidinggevend personeel gemeld. Er zijn responsprocedures om de effecten daarvan te beperken en ervoor te zorgen dat de diensten tijdig operationeel en veilig worden.

Bij ICT-gerelateerde incidenten en significante cyberdreigingen bij het fonds zelf, zorgt het bestuur voor bovengenoemde acties.

De uitbestedingsrelaties informeren BPF Beton over de bovengenoemde aspecten van het beheer van ICT-gerelateerde incidenten en significante cyberdreigingen. Het bestuur cq. de IRM-commissie ontvangt de meldingen, registreert deze, beoordeelt de categorisatie en classificatie en monitort de opvolging. In het geval de ernst van het incident hiertoe aanleiding geeft, zorgt het fonds voor communicatie aan de (gewezen) deelnemers, pensioengerechtigden en werkgevers, voor zover de uitvoeringsorganisatie dit al niet heeft gedaan.

Wanneer een ernstig ICT-gerelateerd incident optreedt en gevolgen heeft voor de financiële belangen van (gewezen) deelnemers, pensioengerechtigden of aangesloten werkgevers, stelt het bestuur hen onverwijld hiervan in kennis. Het bestuur meldt hierbij de maatregelen die zijn genomen om de negatieve gevolgen van een dergelijk incident te beperken.
In het geval van een significante cyberdreiging zal het fonds passende beschermingsmaatregelen onderzoeken en de eventueel getroffenen hiervan op de hoogte stellen.

4.11.2 Datalek

Een zogenaamd ‘datalek’ is een bijzondere vorm van een security incident, waarbij persoonsgegevens betrokken zijn. Datalekken moeten onverwijld binnen 24 uur aan het bestuur van BPF Beton worden gemeld en binnen 72 uur aan de Autoriteit Persoonsgegevens.
Onder datalek verstaan we ieder incident bij verwerking van persoonsgegevens door de pensioenuitvoerder, waarbij sprake is van een inbreuk in verband met persoonsgegevens zoals bedoeld in de Algemene Verordening Gegevensbescherming. Op grond van de AVG dient ieder datalek te worden gemeld, tenzij het niet waarschijnlijk is dat inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.
De pensioenuitvoerder informeert het bestuur bij een datalek over:

- de aard en omvang van de inbreuk op de beveiliging;
- de naam en contactgegevens van degene bij wie meer informatie over de inbreuk kan worden verkregen;
- de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van Persoonsgegevens en (kring van) de betrokkenen;
- de maatregelen die zij heeft getroffen of voorstelt te treffen om de (negatieve) gevolgen van de inbreuk te beperken en te verhelpen;
- aanvullende gegevens die het fonds nodig heeft om een eventuele melding bij de toezichthouder te kunnen verrichten.

Binnen 72 uur beoordeelt het bestuur de melding van een (mogelijk) datalek en bepaalt daarbij of er melding aan de Autoriteit Persoonsgegevens plaats dient te vinden.
Elke melding staat op zich en BPF Beton zal jaarlijks de ervaringen van (gemelde) datalekken evalueren om op grond daarvan te bezien of eenduidige criteria kunnen worden benoemd wanneer er melding aan de AP plaats dient te vinden.

5. Inbedding in integraal risicomanagement

Het informatiebeveiligingsbeleid maakt onderdeel uit van het integraal risicomanagementbeleid van het pensioenfonds. Hiermee is zeker gesteld dat het informatiebeveiligingsbeleid de beleidscyclus doorloopt waarmee ook monitoring en evaluatie terugkeren op de bestuursagenda.

6. Informatie-uitwisseling

Het fonds kan met andere financiële entiteiten informatie en inlichtingen over cyberdreiging uitwisselen, zoals indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratie-instrumenten, voor zover dit:

a) bedoeld is om de digitale operationele weerbaarheid van het fonds te versterken, met name via bewustmaking van cyberdreigingen, beperking of belemmering van de mogelijkheid tot verdere verspreiding van cyberdreigingen, ondersteuning van defensiecapaciteiten, technieken voor dreigingsdetectie, risicobeperkende strategieën en respons- en herstelfasen;
b) gebeurt binnen vertrouwensgemeenschappen van financiële entiteiten;
c) gedaan wordt via regelingen voor informatie-uitwisseling die de potentieel gevoelige aard van de gedeelde informatie beschermen en waarvoor gedragsregels gelden waarin de vertrouwelijkheid van bedrijfsinformatie, de bescherming van persoonsgegevens overeenkomstig Verordening (EU) 2016/679 en de richtsnoeren inzake mededingingsbeleid volledig worden gerespecteerd.

Het fonds stelt de toezichthouder, na goedkeuring van zijn deelname in de vertrouwensgemeenschap, in kennis van de deelname aan de regelingen voor informatie-uitwisseling, en, in voorkomend geval, van de beëindiging van haar deelname zodra deze beëindiging van kracht wordt.

7. Verantwoording

Over de beheersing van informatiebeveiliging legt het pensioenbestuur verantwoording af aan de Raad van Toezicht en informeert het verantwoordingsorgaan.

Op verzoek van de bevoegde autoriteiten verstrekt het bestuur volledige en geactualiseerde informatie over ICT-risico en over hun kader voor ICT-risicobeheer. Aan de bevoegde autoriteit wordt een verslag bezorgd over de evaluatie van het kader voor ICT- risicobeheer indien zij daarom verzoekt. In ieder geval worden zwaarwegende incidenten aan DNB gemeld, zie paragraaf 4.5.1.

In geval van ernstige ICT-gerelateerde incidenten dient het bestuur bij de betreffende toezichthouder het volgende in (middels de daarvoor door de toezichthouder ontwikkelde modellen):

a) een eerste kennisgeving;
b) een tussentijds verslag na de eerste kennisgeving, zodra de status van het oorspronkelijke incident ingrijpend is gewijzigd of de behandeling van het ernstige ICT-gerelateerde incident is gewijzigd op basis van beschikbare nieuwe informatie, in voorkomend geval gevolgd door geactualiseerde kennisgevingen telkens wanneer een relevante actualisering van de status beschikbaar is, alsmede op specifiek verzoek van de bevoegde autoriteit;
c) een eindverslag, wanneer de analyse van de onderliggende oorzaken is voltooid, ongeacht of er reeds beperkende maatregelen zijn uitgevoerd, en wanneer de werkelijke impactcijfers beschikbaar zijn in plaats van ramingen.

Hiertoe wordt alle relevante informatie verzameld en geanalyseerd, worden de verslagen opgesteld en worden de ingevulde modellen ingediend. Indien het technisch niet mogelijk is de eerste kennisgeving met gebruikmaking van het model in te dienen, worden alternatieve middelen

gebruikt om de toezichthouder in kennis te stellen.
De eerste kennisgeving en verslagen bevatten alle informatie die de toezichthouder nodig heeft om de draagwijdte van het ernstige ICT-gerelateerde incident te bepalen en mogelijke grensoverschrijdende effecten te beoordelen.

Het bestuur meldt significante cyberdreigingen aan de toezichthouder indien deze door het bestuur relevant voor het financiële stelsel worden geacht.

In de jaarverslagen besteedt het bestuur aandacht aan het onderwerp informatiebeveiligingsbeleid, zowel bij de uitbestedingspartijen als in zijn geheel.

8. Bekendmaking beleid

Het informatiebeveiligingsbeleid wordt periodiek onder de aandacht gebracht van het bestuur en de verbonden personen en uitbestedingsrelaties. Het bestuur draagt er zorg voor dat iedere nieuwe verbonden persoon bij infunctietreding de beschikking heeft over het informatiebeveiligingsbeleid van het pensioenfonds. Een wijziging van dit beleid communiceert BPF Beton schriftelijk aan hen op wie het beleid van toepassing is. Daarnaast publiceert het fonds het informatiebeveiligingsbeleid op de website.

9. Inwerkingtreding beleid

Het informatiebeveiligingsbeleid is voor het laatst vastgesteld in de bestuursvergadering van …. Het informatiebeveiligingsbeleid is gewijzigd door het IT-beleid te integreren in het informatiebeveiligingsbeleid. Het IT-beleid V3 d.d. december 2021 komt hiermee te vervallen. Het informatiebeveiligingsbeleid is vastgesteld door het bestuur op ….

Bijlage 1 – BIV-classificatie

Beschikbaarheid			
Classificatie	Niveau	Typering	Omschrijving
1	Laag	Relevant	Informatie dient over het algemeen beschikbaar te zijn. Niet-beschikbaarheid is beperkt acceptabel.
2	Gemiddeld	Noodzaak	Informatie dient bijna altijd beschikbaar te zijn.
3	Hoog	Prioriteit	Uitval van informatie alleen in geval van calamiteiten.

Integriteit			
Classificatie	Niveau	Typering	Omschrijving
1	Laag	Geborgd	Basis voor een juist bedrijfsproces met betrekking tot Integriteit. Fouten zijn beperkt toelaatbaar.
2	Gemiddeld	Prominent	Het bedrijfsproces is bijna foutloos.
3	Hoog	Onvoorwaardelijk	Het bedrijfsproces is foutloos.

Vertrouwelijk			
Classificatie	Niveau	Typering	Omschrijving
1	Laag	Confidentieel	Informatie is toegankelijk voor geselecteerde groep van: verbonden personen en medewerkers van een uitbestedingsrelatie. Autorisatierechten worden functiegericht toegekend.
2	Gemiddeld	Vertrouwelijk	Informatie is alleen toegankelijk voor specifiek geselecteerde groep van: verbonden personen en medewerkers van een uitbestedingsrelatie. Autorisatierechten worden functiegericht toegekend.
3	Hoog	Geheim	Informatie is geheim, alleen een beperkt aantal verbonden personen en medewerkers van een uitbestedingsrelatie verkrijgen toegang. Autorisatierechten wordt individueel toegekend.

De classificaties op hoofdcategorieën gelden voor de onderliggende subcategorieën, tenzij anders is ingevuld				
Type	B	I	V	Omschrijving
Bestuursgegevens	1	2	2	Met name beschikbaar voor bestuursonder-steuning en relatiebeheer
NAW				
Identiteit				
06				
Communicatie DNB/AFM				
Communicatie				
Fondsgegevens	2	1	2	Beschikbaar voor Bestuur en adviesdiensten
Uitbestedingscontracten				
DVO/SLA				
Vacatievergoedingen				Alleen op totaalniveau inzichtelijk t.b.v. be-lastingaangifte
Deelnemersinformatie				
Werkgeversinformatie				
Website-informatie			1	
KvK				
Kosten	2	2	1	Zowel administratie als vermogensbeheer
Jaarrekening			1	
Geldstromen				In- en excasso
Deelnemersgegevens	3	1	2	Met name beschikbaar voor medewerkers van pensioenuitvoerder
Persoonsgegevens				
Financiële gegevens				Belastinginformatie
Dienstverbanden				
Arbeidsongeschiktheid		2		
Partner(s) en kinderen				
Uitkeringen		2		
Aanspraken				
Bankgegevens		2		
Werkgeversgegevens	2	2	2	Met name beschikbaar voor medewerkers van pensioenuitvoerder
NAW				
Loonheffingsnummer				
Bankrekeningnummer				
Incasso-informatie				
KvK				
Beleggingsgegevens	2	2	2	Met name beschikbaar voor medewerkers van vermogensbeheerders, fiduciair en be-leggingsadviseur
Beleggingsbeleid				
Strategisch/Tactisch				
Overeenkomsten				
Mandaten				

Bijlage 2 - DNB good practice Informatiebeveiliging 2023

	Governance
1	Define an information security plan
1.1	Information security plan
1.2	IT policies management
2	Define the information architecture
2.1	Enterprise information architecture model
2.2	Data classification scheme
3	Determine technological direction
3.1	Monitor future trends and regulations
3.2	Technology trends
4	Assess and manage (IT) risks
4.1	IT risk management framework
4.2	Risk assessment
4.3	Maintenance and monitoring of a risk action plan
	Organisation
5	Information security organization
5.1	Responsibility for risk, security and compliance
5.2	Management of information security
6	Data and system ownership
6.1	Data and system ownership
7	Manage segregation of duties
7.1	Segregation of duties
	People
8	Manage IT human resources
8.1	Personnel recruitment and retention
8.2	Personnel competences
8.3	Dependence upon individuals
8.4	Personnel clearance procedures
8.5	Job change and termination
9	Ensure operations and use
9.1	Knowledge transfer to end users
9.2	Knowledge transfer to operations and support staff
9.3	Employee awareness
	Processes
10	Change management
10.1	Change standards and procedures
10.2	Impact assessment, prioritization and authorization
10.3	Test environment
10.4	Testing of changes
10.5	Promotion to production
11	Continuity management
11.1	IT continuity plans
11.2	Testing of the IT continuity plan

11.3	Offsite backup storage
11.4	Backup and restoration
12	Manage data
12.1	Storage and retention arrangements
12.2	Disposal
12.3	Security requirements for data management
13	Configuration management
13.1	Configuration repository and baseline
13.2	Identification and maintenance of configuration items
14	Manage third party and supplier services
14.1	Monitoring and reporting of SLA's
14.2	Supplier risk management
15	Incident management
15.1	Security incident definition
15.2	Incident escalation
16	Monitoring
16.1	Security testing, surveillance and monitoring
16.2	Monitoring of internal control framework
16.3	Internal control of third parties
16.4	Evaluation of compliance with external requirements
16.5	Independent assurance
17	User account management
17.1	Identity management
17.2	User account management
	Technology
18	Secure infrastructure
18.1	Infrastructure resource protection and availability
18.2	Infrastructure maintenance
18.3	Cryptographic key management
18.4	Network security
18.5	Exchange of sensitive data
19	Manage malware attacks
19.1	Malicious software prevention, detection and correction
19.2	Vulnerability management (newly identified vulnerabilities)
19.3	Life cycle management
20	Protect infrastructure components
20.1	Protection of security technology
	Facilities
21	Physical security
21.1	Physical security measures
21.2	Physical access
	Testing
22	Testing
22.1	Penetration testing and ethical hacking

Bijlage 3 – controles DORA artikel 9 tot en met 14

Hoofdstuk 3 van DORA (met de voor het fonds relevante artikelen 9 tot en met 14) behandelt de uitvoering van het risicobeheer. Aangezien BPF Beton eindverantwoordelijk is, wordt gecontroleerd of de uitbestedingsrelaties die (belangrijke) ICT-systemen in beheer hebben en gebruiken ten behoeve van het fonds aan de eisen van DORA voldoen. De controles zijn verdeeld in:

- Controles die bij invoering van dit informatiebeveiligingsbeleid worden gedaan en vervolgens periodiek herhaald worden bijvoorbeeld bij contractsvernieuwing.
- Controles waarvoor de uitbestedingsrelatie regelmatig dient te rapporteren.

Eenmalige, periodiek te herhalen controles

Het fonds controleert of (in voldoende mate) (tussen haakjes het nummer van het betreffende artikel van DORA):

- de uitbestedingsrelaties de effecten van ICT-risico op ICT-systemen beperken door de inzet van passende ICT-beveiligingsinstrumenten, -beleidslijnen en -procedures. (9.1)

- het ontwerp, de aanbesteding en de uitvoering van ICT-beveiligingsbeleidslijnen, -procedures, -protocollen en -instrumenten gericht zijn op de waarborging van de weerbaarheid, continuïteit en beschikbaarheid van ICT-systemen, met name die welke kritieke of belangrijke functies ondersteunen, en op de handhaving van hoge normen inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens, zowel in rusttoestand, bij gebruik als bij doorvoer. Hiertoe dienen de uitbestedingsrelaties gebruik te maken van ICT-technologieën en -processen die:
    - de beveiliging van de middelen voor overdracht van gegevens waarborgen;
    - het risico beperken op aantasting of verlies van gegevens, ongeoorloofde toegang en technische gebreken die de bedrijfsactiviteit kunnen belemmeren;
    - een gebrek aan beschikbaarheid, de aantasting van de authenticiteit en integriteit, de inbreuken op de vertrouwelijkheid en het verlies van gegevens voorkomen;
    - ervoor zorgen dat gegevens worden beschermd tegen risico's bij het gegevensbeheer, met inbegrip van slecht bestuur, risico's bij de verwerking en menselijke fouten.

  (9.2 en 9.3)

- de uitbestedingsrelaties een beleid hebben en documenteren inzake informatiebeveiliging waarin regels worden vastgesteld ter bescherming van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens, informatie- en ICT- activa, inclusief die van hun klanten. (9.4a)

- de uitbestedingsrelaties op grond van een op risico's gebaseerde aanpak een degelijke structuur voor netwerk- en infrastructuurbeheer hanteren met gebruik van passende technieken, methoden en cyberaanvallen de getroffen informatieactiva te isoleren en de netwerkaansluitinfrastructuur onmiddellijk kan worden afgekoppeld of gesegmenteerd teneinde besmetting te beperken en te voorkomen, met name voor onderling gekoppelde financiële processen. (9.4b)

- de uitbestedingsrelaties een beleid voeren waarbij de fysieke of logische toegang tot informatie- en ICT-activa wordt beperkt tot hetgeen alleen voor legitieme en goedgekeurde functies en activiteiten noodzakelijk is, en voeren daartoe een reeks beleidslijnen, procedures en controles in om toegangsrechten en een degelijk beheer daarvan te waarborgen. (9.4c)

- de uitbestedingsrelaties beleidslijnen en protocollen hebben voor strenge authenticatiemechanismen die gebaseerd zijn op relevante normen, specifieke controlesystemen en beschermingsmaatregelen voor cryptografische sleutels, waarbij gegevens worden versleuteld uitgaande van de resultaten van goedgekeurde processen van gegevensclassificatie en ICT- risicobeoordeling. (9.4d)

- de uitbestedingsrelaties gedocumenteerde beleidslijnen, procedures en controles hebben voor het beheer van veranderingen in ICT, met inbegrip van veranderingen in software, hardware, firmwarecomponenten, systemen of beveiligingsparameters, die uitgaan van een op risicobeoordeling gebaseerde aanpak en integrerend deel uitmaken van het algemene veranderingsbeheerproces van de uitbestedingsrelatie, teneinde te garanderen dat alle veranderingen in ICT-systemen op gecontroleerde wijze worden geregistreerd, getest, beoordeeld, goedgekeurd, ingevoerd en geverifieerd. (9.4e)

- het beheerproces van de uitbestedingsrelaties inzake ICT-veranderingen goedgekeurd wordt door passende beheerlijnen en voorzien van specifieke protocollen. (9.4e)

- de uitbestedingsrelaties over een passend en alomvattend gedocumenteerd beleid voor patches en updates beschikken. (9.4f)

- de uitbestedingsrelaties over mechanismen beschikken om afwijkende activiteiten zoals ICT-gerelateerde incidenten en significante cyberdreigingen zo spoedig mogelijk te detecteren, met inbegrip van kwesties op het gebied van ICT-netwerkprestaties en ICT-gerelateerde incidenten, en om potentiële zwakke fysieke punten (“single points of failure”) te identificeren. Deze detectiemechanismen dienen regelmatig te worden getest, maken meerdere controlelagen mogelijk en bepalen waarschuwingsdrempels en criteria om processen voor respons op ICT-gerelateerde incidenten in werking te stellen, met inbegrip van automatische waarschuwingsmechanismen voor de betrokken personeelsleden die belast zijn met de respons op ICT- gerelateerde incidenten. (10.1 en 10.2)

- de uitbestedingsrelaties die data rapporteren over systemen beschikken die transactiemeldingen doeltreffend op volledigheid kunnen controleren, omissies en aperte fouten kunnen opsporen en om hernieuwde transmissie van die meldingen kunnen verzoeken. (10.4)

- de uitbestedingsrelaties een alomvattend ICT-bedrijfscontinuïteitsbeleid voeren dat kan worden aangenomen als een specifiek beleid en een integrerend onderdeel vormt van het ruimere bedrijfsbrede beleid inzake bedrijfscontinuïteit van de financiële entiteit. Dit beleid dient te worden uitgevoerd via specifieke, aangepaste en gedocumenteerde regelingen, plannen, procedures en mechanismen die erop gericht zijn:
    - de continuïteit van de kritieke of belangrijke functies van de uitbestedingsrelatie te verzekeren;
    - op een snelle, passende en doeltreffende wijze een respons en een oplossing te bieden voor alle ICT-gerelateerde incidenten waarbij de schade wordt beperkt en prioriteit wordt verleend aan de hervatting van de activiteiten en aan herstelmaatregelen;
    - onverwijld specifieke plannen in werking te stellen om inperkingsmaatregelen, -processen en -technologieën mogelijk te maken die aangepast zijn aan elk type ICT-gerelateerd incident en waarmee verdere schade kan worden voorkomen, alsmede op maat gesneden respons- en herstelprocedures;
    - de voorlopige effecten, schade en verliezen te ramen;
    - maatregelen voor communicatie en crisisbeheersing op te stellen die garanderen dat aan het fonds geactualiseerde informatie wordt verstrekt en verslag uit te brengen aan de bevoegde autoriteiten.

(11.1 en 11.2)

- de uitbestedingsrelaties ICT-respons- en herstelplannen hebben die aan onafhankelijke interne audits worden onderworpen. (11.3)

- de uitbestedingsrelaties passende ICT-bedrijfscontinuïteitsplannen hebben, deze handhaven en voor periodieke tests zorgen, met name wat betreft kritieke of belangrijke functies die zijn uitbesteed of via contractuele overeenkomsten met derde aanbieders van ICT-diensten zijn overeengekomen. (11.4)

- de uitbestedingsrelaties in het kader van het algemene bedrijfscontinuïteitsbeleid een bedrijfsimpactanalyse (business impact analysis — BIA) uitvoeren van hun blootstelling aan ernstige verstoringen van de bedrijfsactiviteiten. Daarin dienen zij de potentiële gevolgen van ernstige verstoringen van de bedrijfsactiviteiten te beoordelen aan de hand van kwantitatieve en kwalitatieve criteria, in voorkomend geval met behulp van interne en externe gegevens en scenarioanalyse. Er dient rekening te worden gehouden met de kritieke aard van geïdentificeerde en in kaart gebrachte bedrijfsfuncties, ondersteuningsprocessen, afhankelijkheden van derden en informatieactiva, en hun onderlinge afhankelijkheden. ICT-activa en ICT-diensten moeten worden ontworpen en gebruikt in volledige overeenstemming met de BIA, met name om de redundantie van alle kritieke onderdelen adequaat te waarborgen. (11.5)

- de uitbestedingsrelaties ten minste jaarlijks en in geval van substantiële wijzigingen in ICT-systemen die kritieke of belangrijke functies ondersteunen de ICT-bedrijfscontinuïteitsplannen en de ICT-respons- en herstelplannen met betrekking tot ICT-systemen die kritieke of belangrijke functies ondersteunen, testen, alsmede de crisiscommunicatieplannen. In de testplannen moeten scenario's opgenomen worden van cyberaanvallen en omschakelingen tussen de primaire ICT-infrastructuur en de reservecapaciteit, backups en reservefaciliteiten die noodzakelijk zijn om te voldoen aan de in artikel 12 bedoelde verplichtingen. (11.6)

- de uitbestedingsrelaties regelmatig hun ICT-bedrijfscontinuïteitsbeleid en hun ICT-respons- en herstelplannen evalueren, rekening houdend met de resultaten van de tests en de aanbevelingen die voortvloeien uit audits of toezichtbeoordelingen. (11.6)

- de uitbestedingsrelaties over een functie voor crisisbeheer beschikken die in geval van activering van hun ICT-bedrijfscontinuïteitsplannen of ICT-respons- en herstelplannen onder meer duidelijke procedures bepaalt voor het beheer van interne en externe crisiscommunicatie. (11.7)

- de uitbestedingsrelaties gemakkelijk toegankelijke registers bijhouden van hun activiteiten vóór en tijdens storingen wanneer hun ICT-bedrijfscontinuïteitsplannen en ICT-respons- en herstelplannen worden geactiveerd. (11.8)

- de uitbestedingsrelaties een back-upbeleid en -procedures (waarin nader wordt bepaald op welke gegevens de back-up en de minimale frequentie van de back-up worden toegepast, op basis van het kritieke karakter van de informatie of het vertrouwelijkheidsniveau van de gegevens) en terugzettings- en herstelprocedures en -methoden hebben en documenteren. Dit heeft ten doel het terugzetten van ICT-systemen en gegevens te verzekeren met een minimale uitval en een beperkte verstoring en beperkt verlies. (12.1)

- de uitbestedingsrelaties back-upsystemen hebben die kunnen worden geactiveerd in overeenstemming met het back-upbeleid, de back-upprocedures, en de terugzettings- en

herstelprocedures en -methoden. De activering van backupsystemen mag de beveiliging van de netwerk- en informatiesystemen of de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens niet in gevaar brengen. De back-upprocedures en de terugzettings- en herstelprocedures en -methoden moeten periodiek worden getest. (12.2)

- de uitbestedingsrelaties van ICT-systemen die fysiek of logisch gescheiden zijn van het bron-ICT-systeem gebruik maken wanneer zij back-upgegevens terugzetten met behulp van eigen systemen. De ICT-systemen dienen tegen ongeoorloofde toegang of beschadiging van ICT beveiligd te zijn en het mogelijk te maken diensten indien nodig tijdig terug te zetten met gebruikmaking van gegevens en systeemback-ups. (12.3)

- de uitbestedingsrelaties bij het bepalen van de doelstellingen inzake hersteltijd en herstelpunt voor elke functie rekening houden met de vraag of het een kritieke of belangrijke functie betreft en met het potentiële algemene effect op de marktefficiëntie. Deze tijdsdoelstellingen zorgen ervoor dat de overeengekomen niveaus in extreme scenario's worden gehaald. (12.6)

- de uitbestedingsrelaties bij herstel van een ICT-gerelateerd incident de benodigde controles verrichten, ook meerdere controles, waaronder afstemmingen, om ervoor te zorgen dat het hoogste niveau van gegevensintegriteit wordt gehandhaafd. Deze controles dienen ook te worden verricht bij het reconstrueren van gegevens van externe belanghebbenden om te waarborgen dat alle gegevens consistent zijn tussen de systemen. (12.7)

- in het ICT-risicobeoordelingsproces van de uitbestedingsrelaties voortdurend naar behoren rekening wordt gehouden met lessen die voortspruiten uit de uitgevoerde tests op de digitale operationele weerbaarheid en uit ICT-gerelateerde incidenten die zich in het reële leven hebben voorgedaan, met name cyberaanvallen, alsmede met problemen die zich voordoen bij de activering van ICT-bedrijfscontinuïteitsplannen en ICT-respons- en -herstelplannen, samen met relevante informatie die met tegenpartijen wordt uitgewisseld en tijdens toetsingen in het toezicht worden beoordeeld. Die bevindingen dienen de basis te vormen voor passende herzieningen van relevante onderdelen van het kader voor ICT-risicobeheer van de uitbestedingsrelatie. (13.3)

- de uitbestedingsrelaties erop toezien dat hun strategie voor digitale operationele weerbaarheid op doeltreffende wijze wordt uitgevoerd. Zij dienen de ontwikkeling van ICT-risico's in de tijd te inventariseren en de frequentie, de types, de omvang en de evolutie van ICT-gerelateerde incidenten, met name cyberaanvallen en de patronen daarvan, te analyseren om inzicht te krijgen in het niveau van blootstelling aan ICT-risico's, met name met betrekking tot kritieke of belangrijke functies, en de maturiteit en paraatheid van de financiële entiteit ten aanzien van deze risico's te verhogen. (13.4)

- het leidinggevend ICT-personeel van de uitbestedingsrelatie ten minste jaarlijks verslag uitbrengt bij het leidinggevend orgaan van de uitbestedingsrelatie over de hierboven bij 13.3 genoemde bevindingen en aanbevelingen doet. (13.5)

- de uitbestedingsrelaties bewustmakingsprogramma's uitvoeren op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid als verplichte modules in de opleidingsprogramma's voor het personeel. Die programma's en opleidingen dienen van toepassing te zijn op alle werknemers en hoger leidinggevend personeel, en een niveau van complexiteit te hebben dat in verhouding staat tot hun takenpakket. In voorkomend geval dienen zij ook derde aanbieders van ICT-diensten op in hun relevante opleidingsprogramma's. (13.6)

- de uitbestedingsrelaties voortdurend toezicht houden op relevante technologische ontwikkelingen, ook om inzicht te krijgen in de mogelijke effecten van de invoering van deze nieuwe technologieën op de ICT-beveiligingsvereisten en de digitale operationele weerbaarheid en zich op de hoogte houden van de meest recente processen voor ICT-risicobeheer, om bestaande of nieuwe vormen van cyberaanvallen doeltreffend aan te pakken. (13.7)

- de uitbestedingsrelaties als onderdeel van het kader voor ICT-risicobeheer over crisiscommunicatieplannen beschikken die het mogelijk maken ten minste ernstige ICT-gerelateerde incidenten of kwetsbaarheden op verantwoordelijke wijze bekend te maken aan cliënten en tegenpartijen en, in voorkomend geval, aan het publiek. (14.1)

- de uitbestedingsrelaties een communicatiebeleid voor het interne personeel en externe belanghebbenden voeren als onderdeel van het kader voor ICT-risicobeheer. In dat communicatiebeleid voor het personeel dient rekening te worden gehouden met de noodzaak om een onderscheid te maken tussen personeel dat betrokken is bij het ICT-risicobeheer, met name het personeel dat verantwoordelijk is voor respons en herstel, en personeel dat moet worden geïnformeerd. (14.2)

Controles op basis van regelmatige rapportages

Het fonds controleert of (in voldoende mate) (tussen haakjes het nummer van het betreffende artikel van DORA):

- de uitbestedingsrelaties de beveiliging en werking van de ICT-systemen en -instrumenten monitoren en controleren. (9.1)

- de uitbestedingsrelaties voldoende middelen en capaciteiten inzetten om toezicht te houden op activiteiten van gebruikers en het optreden van ICT-anomalieën en ICT-gerelateerde incidenten, met name cyberaanvallen. (10.3)

- de uitbestedingsrelaties ICT-capaciteiten in reserve houden met middelen, capaciteiten en functies die geschikt zijn om te voorzien in de zakelijke behoeften. (12.4)

- de uitbestedingsrelaties over capaciteiten en personele middelen beschikken om informatie te verzamelen over kwetsbaarheden en cyberdreigingen, ICT-gerelateerde incidenten, met name cyberaanvallen, en om de waarschijnlijke gevolgen ervan voor hun digitale operationele weerbaarheid te analyseren. (13.1)

- de uitbestedingsrelaties ICT-gerelateerde post-incidentevaluaties verrichten na verstoringen van hun kernactiviteiten ten gevolge van een ernstig ICT-gerelateerd incident, daarbij de oorzaken van de verstoring analyseren en de verbeteringen identificeren die moeten worden aangebracht in de ICT-activiteiten of in het kader van het ICT-bedrijfscontinuïteitsbeleid In deze evaluaties dient te worden bepaald of de vastgestelde procedures zijn gevolgd en of de genomen maatregelen doeltreffend zijn geweest, onder meer met betrekking tot:
    - de snelheid waarmee is gereageerd op veiligheidswaarschuwingen en de effecten en de ernst van ICT-gerelateerde incidenten zijn vastgesteld;
    - de kwaliteit en de snelheid bij het verrichten van een forensische analyse, indien deze passend wordt geacht;
    - de doeltreffendheid van incidentescalatie binnen de uitbestedingsrelatie;
    - de doeltreffendheid van interne en externe communicatie.

  (13.2)

Daarnaast ontvangt het fonds rapportages van de uitbestedingsrelaties en evalueert deze over het beleid, de maatregelen en de effectiviteit daarvan hierboven genoemd bij de DORA-artikelen:

- 9.4b en 9.4c
- 10.1, 10.2 en 10.4
- 11.1 tot en met 11.6
- 12.2, 12.3 en 12.7
- 13.3 en 13.4