VAN LANSCHOT KEMPEN

INVESTMENT MANAGEMENT

Non-Financial Risk Rapportage - Q3-2024

Inhoudsopgave

Inleiding & context

Voor u ligt het VLK IM Non-Financial Risk (NFR) Klantrapport voor het derde kwartaal van 2024. Dit rapport biedt een gedetailleerd overzicht van de belangrijkste niet-financiële risico's die onze organisatie in de afgelopen periode heeft geïdentificeerd en beheerd. Het doel van dit rapport is om onze institutionele klanten inzicht te geven in de belangrijkste ontwikkelingen, risico-items per risicocategorie en de mate van risicobeheersing. Daarnaast bespreken we de voortgang van de integratie van de WTP-dienstverlening en de voortgang van de implementatie van DORA.
Wij hopen dat dit rapport u een helder beeld geeft van onze inspanningen op het gebied van risicobeheer en de stappen die wij nemen om de risico's binnen onze dienstverlening te minimaliseren.

Rapportopbouw

Elke risicocategorie in dit rapport wordt eerst gedefinieerd. Per categorie wordt (exceptiegericht) inzicht gegeven in de belangrijkste risico-items, hoe deze van toepassing zijn en de mate van beheersing daarvan. Non-Financial Risk Management (hierna: "NFRM") coördineert en stelt dit rapport op met input van de eerste lijn[1]. NFRM en Compliance dragen zorg voor balans en nuance door middel van onafhankelijke monitoring van beheersmaatregelen en risicobeoordelingen en geven hierbij hun perspectief op het risicoprofiel van Van Lanschot Kempen Investment Management (hierna: "VLK IM"). De beleidsdocumenten die relevant zijn voor VLK IM zijn, gegroepeerd per onderwerp, opgenomen in bijlage IV.

Connectie VLK IM NFR klantrapport en dienstenmatrix

De dienstenmatrix voor institutionele klanten biedt inzicht in de verschillende diensten die kunnen worden afgenomen door klanten bij VLK IM. Institutionele klanten met fiduciair management en/of alternative investment solutions dienstverlening verkrijgen hierdoor eenvoudiger inzicht in welke risico's op welke wijze op hen van toepassing zijn en in welke mate de hieraan gekoppelde beheersmaatregelen effectief zijn. Vooruitlopend op de WTP transitie zal per eind 2024 ook de WTP dienstverlening voor pensioenfondsen worden geïntegreerd in de dienstenmatrix. Afhankelijk van de transitiedatum zal dit per klant worden afgestemd bij de reguliere update van de dienstenmatrix (zie tevens de toelichting over WTP in bijlage I).

Risicotaxonomie

De risicotaxonomie in het NFR klantrapport is per 1 januari 2024 gewijzigd van de FIRM-risicocategorieën naar de risicotaxonomie die gehanteerd wordt door VLK IM. De risicotaxonomie van VLK IM is gebaseerd op de ORX-taxonomie, aangevuld met het Integrity/Compliance risico en het Legal risico. ORX is een industrie brede standaard die wereldwijd wordt gebruikt door de grootste banken en omvat de huidige scope van de Basel taxonomie. De taxonomie wordt periodiek bijgewerkt door haar leden en volgt daarmee de laatste ontwikkelingen op het gebied van non-financial risk management.

Risicobereidheid en risicobeheersing

VLK IM herijkt jaarlijks haar risicoprofiel in een risicobeoordeling, waarin VLK IM een inschatting maakt van de belangrijkste niet-financiële risico's van haar dienstverlening en de mate waarin VLK IM bereid is het risico te accepteren. Deze herijking vindt plaats door op groepsniveau risicolimieten vast te stellen, deze te vertalen naar onderliggende bedrijfsonderdelen en het geheel te laten goedkeuren op bestuursniveau. Dit heeft geleid tot enkele wijzigingen die tot uiting komen in het NFR Dashboard. De doelstelling is om per risicotype vast te stellen hoeveel risico acceptabel is. VLK IM neemt aanvullende maatregelen wanneer vastgesteld wordt dat het restrisico buiten de vastgestelde risicobereidheid valt. De relevante beheersmaatregelen zijn vastgelegd in het beheersingsraamwerk van VLK IM. Bijlage III toont de van toepassing zijnde risicocategorieën, definities en

[1] Binnen VLK IM wordt het 'three lines of defence' model toegepast waarin:
- De eerste lijnafdelingen eigenaar zijn van de beheersing en verantwoordelijk voor de uitvoer hiervan ('risk takers');
- De eerste lijnafdeling Internal Control de eerste lijn ondersteunt bij de implementatie van risicomanagement en compliance-gerelateerde onderwerpen;
- De tweede lijnafdelingen, Risk Management en Compliance, de onafhankelijke toetsing van de beheersing verzorgen ('risk challengers');
- En de derde lijnafdeling, Internal Audit, onafhankelijke audits en thema-onderzoeken uitvoert in opdracht van het VLK IM management ('risk assurers').

impactclassificatie.VLK IM heeft voor het risicotype transaction processing & (change) execution gekozen voor een hogere risicobereidheid. De hogere risicobereidheid heeft betrekking op één van de vijf subrisico's[2], namelijk het change execution risico. VLK IM investeert momenteel in verandertrajecten zoals het Accelerate programma waar de WTP-implementatie, het rationaliseren van onze fondsen en het versterken van onze IT-systemen onderdelen van zijn. Deze veranderingen komen ten goede van onze klanten, maar brengen ook risico's met zich mee. De omvang en complexiteit van deze veranderingen resulteren in een tijdelijk hoger inherent risico. Het aangaan van dit risico is vertaald in een tijdelijk hogere risicobereidheid. Het verhoogde inherente risico wordt geadresseerd met extra beheersingsmaatregelen. Voor de overige subrisico's onder het risicotype transaction processing & (change) execution geldt een beperkte risicobereidheid.

Scope en positionering rapport

Dit NFR-klantrapport beoogt met name institutionele (fiduciair management) klanten van VLK IM inzicht te bieden in de beheersing van niet-financiële risico's. Dit rapport betreft het perspectief van de tweedelijns Non-Financial Riskfunctie en is aanvullend op de ISAE 3402 rapportage. De ISAE 3402 rapportage betreft de externe onafhankelijke Assurance op de interne beheersmaatregelen bij een serviceorganisatie. VLK IM vervult deze rol richting haar institutionele klanten doordat VLK IM vermogen beheert. Dit rapport onderscheidt de volgende niet-financiële risicocategorieën:

1. People risk;
2. Physical Security & Safety risk;
3. External Fraud risk;
4. Internal Fraud risk;
5. Business Continuity risk;
6. Transaction processing and (change) execution risk;
7. Technology risk;
8. Third Party risk;
9. Information Security risk;
10. Statutory reporting and tax risk;
11. Data Management risk;
12. Integrity-/Compliance risk;
13. Legal risk.

Dit rapport is toegespitst op de fiduciaire en alternative investment solutions dienstverlening aan klanten van VLK IM. Van Lanschot Kempen N.V. heeft beleidsdocumenten en procedures opgesteld die gelden voor de gehele Van Lanschot Kempen groep (hierna: "VLK"), inclusief VLK IM. Voor dit rapport zijn de perspectieven vanuit NFRM en Compliance van belang. Dit betreffen groepsfuncties. Inzichten opgenomen in dit rapport hebben enkel betrekking op de mate van beheersing binnen VLK IM.

Disclaimer: geen onafhankelijke Assurance

De VLK IM Non-Financial Risk rapportage wordt door NFRM (tweede lijn) opgesteld en met de VLK IM board (eerste lijn) periodiek gedeeld en besproken. Dit rapport is informatief van aard en stelt onze klanten in staat om zich een beeld te vormen over de beheersing van de niet-financiële risico's door VLK IM. Op dit rapport is geen onafhankelijke Assurance afgegeven. De inhoud van dit rapport is vertrouwelijk en dient als zodanig te worden behandeld. Verspreiding van dit rapport, of inhoud daarvan, aan derden is slechts toegestaan na voorafgaande toestemming van VLK IM.

[2] Het transaction processing & (change) execution risk is verdeeld in de volgende 5 subrisico-categorieën: Processing/execution failure gerelateerd aan (1) klanten en producten, (2) Securities & Collateral, (3) Third parties, (4) Internal operations & (5) Change execution.

NFR Rapportage Q3-2024

Het algehele risicoprofiel voor VLK IM is, per Q3 2024, **beperkt**[3]. Het risicoprofiel is daarmee stabiel ten opzichte van Q2 2024.

Non-Financial Risk Dashboard Q3-2024

Inschatting door NFRM van het netto risico (na geïmplementeerde beheersmaatregelen) per risicodomein.

Risicodomein	Q3-2024	Q2-2024	Q1-2024	Risico bereidheid VLK (Doel)
People risk	🟢	🟢	🟢	🟡
Physical security & safety risk	🟢	🟢	🟢	🟢
External Fraud risk	🟢	🟢	🟡	🟡
Internal Fraud risk	🟢	🟢	🟢	🟢
Business Continuity risk	🟡	🟡	🟡	🟡
Transaction processing & (change) execution risk	🟡	🟡	🟠	🟠
Technology risk	🟢	🟢	🟡	🟡
Third Party risk	🟢	🟢	🟡	🟡
Information security risk	🟡	🟡	🟠	🟡
Statutory reporting & tax risk	🟢	🟢	🟢	🟢
Data management risk	🟡	🟡	🟡	🟡
Integrity-/Compliance risk	🟡	🟡	🟡	🟡
Legal risk	🟢	🟢	🟢	🟡

Legenda risicoprofiel:

- 🟢 Laag
- 🟡 Beperkt
- 🟠 Substantieel
- 🔴 Hoog

[3] VLK IM hanteert voor de bepaling van het algehele risicoprofiel de 'weakest-link' methode. Dit betekent dat het risicodomein met het hoogste risicoprofiel het algehele risicoprofiel bepaald. Zie tevens bijlage III voor de impactclassificatie.

People risk

NFRM beschouwt het People-risico als '**laag'** (groen). In Q3 hebben zich geen incidenten voorgedaan met betrekking tot de medewerkers van VLK IM. Human Resources (HR) monitort de ontwikkelingen binnen de verschillende teams continu en adviseert het Management Team (MT) van VLK IM hier proactief over.
In het derde kwartaal van 2024 is er aandacht besteed aan het voor medewerkers beschikbare aanbod van trainingen. Er is een speciaal samengestelde teambuilding activiteitenbundel voor managers gelanceerd, er is een E-learning over generatieve AI uitgerold en de Inclusion & Bias Awareness Training is voortgezet.
Er was in het afgelopen kwartaal een toename in de doorstroom van medewerkers te zien, alsmede in de diversiteit van nieuwe medewerkers. De mate van verzuim bleef ruim onder het niveau van de CBS benchmark.

Physical security & safety risk

NFRM beschouwt het Physical security & safety-risico als **'laag'** (groen). In Q3 hebben zich geen incidenten voorgedaan met betrekking tot schade aan gebouwen, medewerkers en/of gelieerde personen van VLK IM. Er worden afdoende mitigerende maatregelen genomen, zowel wat betreft de toegang tot panden en het onderhoud ervan, als op het gebied van bedrijfshulpverlening. Er vindt continue monitoring, testing en verbetering plaats.

External fraud risk

NFRM beschouwt het External Fraud-risico als '**laag'** (groen). In Q3 hebben zich geen incidenten voorgedaan met betrekking tot fraude door externe partijen die betrekking hadden op VLK IM. Externe fraude komt bij VLK met name voor bij de private bank, in de vorm van 'bank helpdesk' fraude. VLK monitort voortdurend ontwikkelingen en verbetert zijn mogelijkheden om pogingen tot externe fraude te detecteren, stoppen en/of te herstellen.

Internal fraud risk

NFRM beschouwt het Internal Fraud-risico als '**laag**' (groen). In Q3 hebben zich geen incidenten voorgedaan met betrekking tot fraude door interne medewerkers op VLK IM. VLK heeft beleid en procedures, permanente educatie op het gebied van integriteit en systeemtechnische en procedurele functiescheiding als belangrijkste maatregelen ingericht om interne fraude te helpen voorkomen.

Business continuity risk

NFRM beschouwt het Business continuity-risico als '**beperkt'** (geel). Om het risicoprofiel verder omlaag te brengen werkt VLK dit jaar aan een verbetering van de BIA-methodologie met als doel om beter inzicht te krijgen in de business continuity risico's. De vereisten vanuit de DORA worden hierin meegenomen, zie ook bijlage II. In Q3 heeft zich één P1-incident[4] voorgedaan die een impact heeft gehad op de operationele processen van VLK IM, zie hiervoor de uitleg bij het Technology-risk. De jaarlijkse Business Continuity Analysis is vernieuwd. Hiernaast is uitgebreid aandacht besteed aan het testen van uitwijkprocedures en aan het testen van het tijdig bij elkaar komen van het Crisis Support Team binnen VLK IM.

Transaction processing & (change) execution risk

NFRM beschouwt het transaction processing & (change) execution risico als '**beperkt'** (geel). In Q3 hebben zich geen significante incidenten voorgedaan binnen VLK IM.

Naar aanleiding van het afsluiten van meerdere onderdelen van het Accelerate programma is begin 2024 het interne beheersingsraamwerk verder vernieuwd. De aanscherpingen zien toe op de juistheid en volledigheid van het risicobeheersingsraamwerk in de Governance Risk & Compliance (GRC)-tool (Bwise). In de komende maanden zal het Accelerate programma formeel beëindigd worden en eventuele openstaande onderdelen zullen opgenomen worden in de reguliere project management organisatie.

[4] Een P1-incident is een IT-incident met de hoogste impactclassificatie.

De externe accountant heeft, als onderdeel van de audit op het ISAE-raamwerk over 2023, een schone ISAE-verklaring afgegeven. VLK IM is in samenwerking met Internal Control en NFRM gestart met het verder inzichtelijk maken van het proceslandschap inclusief de relatie met de dienstenmatrix.

Technology risk

NFRM beschouwt het Technology-risk als '**laag'** (groen). In Q3 heeft zich een kritisch IT-incident voorgedaan dat een impact heeft gehad op de IT-systemen van VLK IM. Dit incident werd veroorzaakt doordat de uitwisseling van data tussen on-premise en cloud korte tijd niet mogelijk was, vanwege een overbelaste netwerk connectie doordat er gelijktijdig een andere datamigratie plaatsvond. Dit resulteerde in deels incomplete data voor de Portfolio Managers en het duurde enkele uren voordat de Portfolio Managers en de andere gebruikers weer over de juiste data konden beschikken. Het incident heeft verder geen impact gehad op klanten doordat de ontbrekende data beperkt was. Acties zijn genomen om dergelijke incidenten in de toekomst te voorkomen.

NFRM stelt vast dat er positieve ontwikkelingen plaatsvinden ten aanzien van de beheersing van het Technology-risk. NFRM blijft samen met het eerstelijns management de ontwikkelingen rondom het Technology-risk monitoren. Daarnaast monitort NFRM of de IT-roadmap met bredere IT-ontwikkelingen adequaat wordt doorlopen. Hierbij ziet NFRM dat de business NFRM regelmatig betrekt in deze IT-ontwikkelingen.

In de IT-roadmap is doorlopende aandacht voor levenscyclusonderhoud, security en digitale transformatie van kernprocessen. Voornaamste ontwikkelingen die de komende 12 maanden op de agenda staan zijn – voor zover relevant voor de klantgroep fiduciair management:

- Implementatie van iLevel als systeem voor administratie, analyse en rapportage over alternatieve beleggingen, en het verbeteren van de dataverzamelprocessen met behulp van o.a. serviceproviders, het Canoe platform en IQ/EQ. De dienstverlener IQ/EQ verzamelt en administreert portfolio data (inclusief waarderingen, commitments en cashflow data) ten behoeve van de alternatieve investment solutions mandaten en ontsluit deze data vervolgens richting ilevel.
- Wet Toekomst Pensioenen (WTP): ondersteunen van klanten die vanaf 2025 zullen overgaan op de SPR-regeling. Dit omvat het aansluiten van datastromen conform sectorafspraken, en het aanpassen van bestaande business processen voor de betreffende klanten, zie tevens bijlage I.
- Optimaliseren van de klantrapportages. Dit omvat:
    - Het implementeren van FactSet als systeem voor performance meting en attributie;
    - Het uitrollen van nieuwe interne systemen voor lookthrough rapportages (w.o. ESG) ter vervanging van FactSet;
    - Het uitbreiden van de rapportage functionaliteit in het klantportaal
    - Het moderniseren van de reguliere pdf-rapportages.
    - Het uitbreiden van de managerfactsheets voor nieuwe beleggingscategorieën en diensten, zoals vastgoed en LDI
- Afronden van het modelvalidatie-traject voor interne LDI-rekenmodellen en -tools.
- Uitvoeren van een selectietraject voor het vervangen van de huidige back-, mid- en front-office tooling door een geïntegreerde front-office en mid-office applicatie.

Third party risk

NFRM beschouwt het Third party risico als '**laag'** (groen). VLK IM is 'in control' ten aanzien van uitbestedingen voor fiduciair managementklanten. Er is sprake van beperkte uitbesteding (ook voor niet kernactiviteiten). NFRM beschouwt uitbestedingen in een breder kader als een blijvend aandachtspunt vanwege de wereldwijde toename van cybercrime-incidenten, de globalisering van dataverwerking en zich verlengende procesketens. Daarom wordt door VLK IM, voorafgaand aan een uitbesteding, een risk assessment uitgevoerd om de risico's binnen de keten (onderuitbesteding) te identificeren en vast te stellen welke maatregelen de serviceprovider heeft genomen om deze risico's te mitigeren. Zie voor een overzicht van de (onder)uitbestedingen bijlage V. Het restrisico valt binnen de VLK IM-risicobereidheid.

Information security risk

NFRM beschouwt het Information security-risico als '**beperkt'** (geel). Er is geen aanleiding geweest om het Information security-risico in het derde kwartaal aan te passen c.q. bij te stellen.

Er hebben zich in Q3-2024 geen IT-beveiligingsincidenten hebben voorgedaan. Maatregelen om de geïdentificeerde risico's verder te mitigeren hebben betrekking op:

- Netwerksegmentatie: VLK implementeert momenteel een systeem om netwerksegmentatie verder te versterken en volgt hier het 'least privilege' principe. Ook in Q3 2024 is voor verschillende (kritische) informatiesystemen netwerksegmentatie daadwerkelijk ingericht;
- Implementeren van additionele 'Attack Surface Reduction' maatregelen om de aanvalsoppervlakte voor cyber criminelen te verkleinen met als doel om de risico's rondom Cybercrime verder te mitigeren.
- Misconfiguraties: verschillende initiatieven die zich richten op de belangrijkste configuratieverbeteringen voor het netwerk van VLK. Voortbordurend op het tweede kwartaal 2024 zijn ook in Q3-2024 zijn verschillende verbeteringen gerealiseerd om dergelijke misconfiguraties effectiever te kunnen identificeren en mitigeren. Daarnaast is een aantal nieuwe initiatieven toegevoegd aan deze maatregelen, waaronder een aantal initiatieven die zich primair richten op de cloud.
- Systeem Hardening: eerder in 2024 is een nieuwe roadmap ontwikkeld om Policy Compliance scores voor alle draaiende Operating Systems naar een hoger niveau te brengen. De voortgang van deze roadmap is op schema en voor het komende kwartaal zijn een aantal nieuwe technologieën geselecteerd om ook voor deze technologieën de Policy Compliance scores verder te verbeteren.

Bovenstaande acties zijn opgenomen In een aantal securityprogramma's om de voortgang te monitoren. Tevens zijn er verschillende indicatoren ten aanzien van informatiebeveiliging en (cyber) security geformuleerd, verdeeld over verscheidene risicocategorieën. Deze indicatoren worden vanuit het Corporate Information Security Overleg (CISO) gemonitord en waar noodzakelijk worden initiatieven gestart om verbeteringen te realiseren. Als organisatie heeft VLK continue focus op het verbeteren van informatiebeveiliging. Voortgang op bovenstaande acties heeft een positieve invloed op de risicoclassificatie voor information security.

Statutory reporting & Tax risk

NFRM beschouwt het Statutory reporting & Tax-risico als **'laag'** (groen). In Q3 hebben zich geen incidenten voorgedaan met betrekking tot het (tijdig) rapporteren aan toezichthoudende instanties.

Datamanagement risk

NFRM beschouwt het Data management-risico als '**beperkt**' (geel). In Q3 hebben zich geen kritische Data-incidenten voorgedaan die een impact hebben gehad op de beschikbaarheid en kwaliteit van data binnen VLK IM. Het afgelopen jaar vonden er positieve ontwikkelingen plaats ten aanzien van de beheersing van datamanagement. Hierbij zijn o.a. meer data kwaliteitscontroles geïmplementeerd, waardoor het aantal data-gerelateerde incidenten is gedaald. In Q3 is er een start gemaakt met de ontwikkeling van een rapportage om, over tijd, inzicht te krijgen in de kwaliteit van data binnen VLK IM. NFRM blijft samen met het eerstelijns management de ontwikkelingen rondom datamanagement monitoren.

Data Management is en blijft een belangrijk aandachtspunt binnen VLK IM waarbij de focus ligt op datakwaliteit over de gehele keten. Gedurende 2024 zijn de voornaamste ontwikkelingen gericht op:

- Het continu toevoegen en verbeteren van data kwaliteitschecks in de bronsystemen (continuous monitoring).
- De implementatie van een generiek dashboard dat een totaalbeeld geeft over datakwaliteit.
- Het verder omhoog brengen van het volwassenheidsniveau van datamanagement, onder andere door middel van educatie.

Integrity-/Compliance risk

VLK Compliance beschouwt de voor dit rapport van toepassing zijnde Integrity-/Compliance-risico's[5] over het geheel genomen als '**beperkt**' (geel).

- Aan het begin van het derde kwartaal is mevrouw D. Hendriks, Chief Risk Officer van Van Lanschot Kempen N.V., toegetreden tot de statutaire directie van VLK IM, met Risk als haar aandachtsgebied. Dit waarborgt het belang van en de aandacht voor Risk en Compliance binnen VLK IM.
- Beleidsdocumenten voor relevante gebieden zijn opgesteld en beheersmaatregelen geïmplementeerd. Deze zijn dit kwartaal effectief getest.
- VLK IM is dit kwartaal niet onderworpen geweest aan enige vorm van handhaving of sancties door een regelgevende en/of toezichthoudende instantie die een wezenlijke invloed kan hebben op zijn taken onder de uitvoering van de dienstverlening.
- Er deden zich tijdens het derde kwartaal twee belasting-gerelateerde (operationele) fondsincidenten voor, evenals een fondsliquidatie benodigd als gevolg van belastingvoorschriften. De belastingstatus van VLK IM-fondsen verdient aandacht, aangezien het overtreden van belastingvoorschriften een aanzienlijke impact zou kunnen hebben op zowel de fondsen als de investeerders. VLK IM heeft reeds acties in gang gezet om het 'Tax Control' raamwerk te verbeteren.
- Eind september bleek de gestelde limiet voor het aantal niet tijdig afgeronde CDD-dossierreviews te zijn overschreden, dit is in oktober alsnog verholpen. Er zijn geen andere materiële incidenten of problemen geïdentificeerd op dit gebied gedurende dit kwartaal.

Legal risk

VLK IM beschouwt het Legal risico als '**laag**' (groen). VLK IM is in control ten aanzien van het identificeren en communiceren van relevante (wijzigingen in) wetgeving. De juridische afdeling van VLK zit daarnaast dicht op de commerciële activiteiten en is nauw betrokken bij de dienstverlening, vanuit een adviserende rol. In dat kader heeft VLK IM dit jaar o.a. een eerste analyse gedaan op de Digital Operational Resilience Act (hierna: de 'DORA') om vast te stellen of het huidige beleid, standaarden en procedures voldoen. Hieruit kan geconcludeerd worden dat VLK IM op hoofdlijnen voldoet. De verdere implementatie is als project opgepakt om tijdig te voldoen aan de DORA, zie tevens bijlage II. Het restrisico valt binnen de VLK IM-risicobereidheid.

[5] Zie voor definitie appendix IV

Bijlage I: WTP

VLK IM is klaar voor de operationele servicing van WTP-klanten. Dit geldt zowel voor klanten die kiezen voor de Flexibele Premieregeling (FPR) als voor klanten die kiezen voor de Solidaire Premieregeling (SPR). Er wordt nu nog gewerkt aan verfijning van de SPR-dienstverlening, zo wordt in Q4 de laatste hand gelegd aan de plausibiliteitschecks op de data die we verwachten te ontvangen van de Pensioen Uitvoeringsorganisaties (PUOs). De verwachting was dat een koploperklant per 1 januari 2025 over zou gaan naar de SPR, maar deze transitie is uitgesteld. De eerste transitie naar de SPR van een VLK IM klant staat nu gepland voor 1 juli 2025.

De dienstverlening voor klanten die kiezen voor de FPR is vergelijkbaar met de dienstverlening voor onze huidige Collectieve Individual Defined Contribution (CIDC) klanten, dus daarvoor hoeven geen directe wijzigingen plaats te vinden in de dienstverlening. Met een aantal (toekomstige) FPR-klanten is VLK IM in gesprek over het omzetten van de datafeed naar de Sivi-standaard.

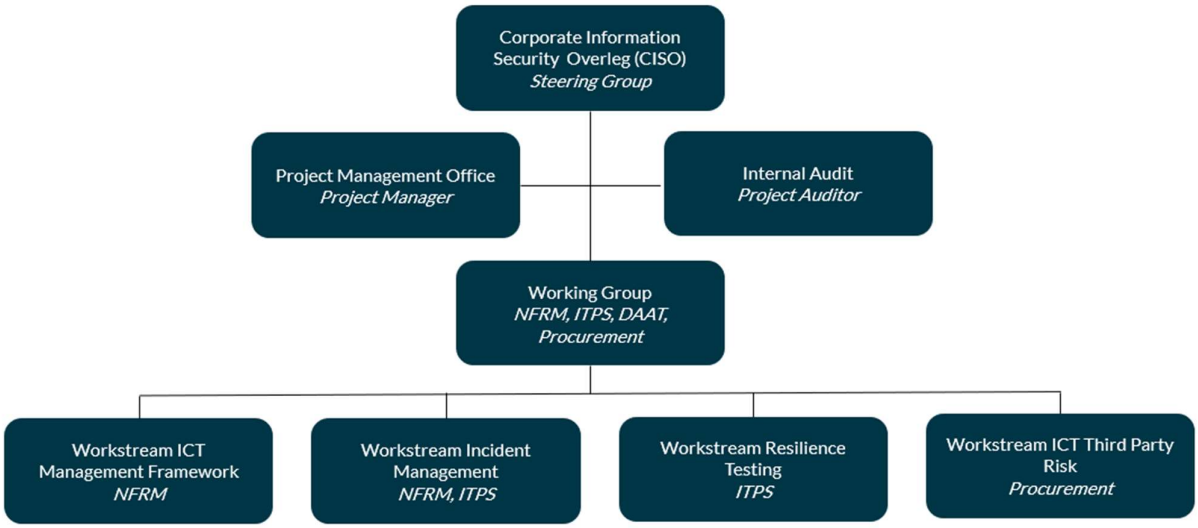
Voor klanten die kiezen voor de Solidaire Premieregeling is de nieuwe dienstverlening opgezet. VLK IM is gereed om via een API-connectie maandelijks van pensioenadministrateurs (PUO's) drie informatiestromen (1a, 1b en 1c) in JSON-format te ontvangen en in te lezen. Op basis van informatiestroom 1a, met de vermogens per cohort, kan VLK IM maandelijks de normallocatie naar de rendements- en de matchingportefeuille met bijbehorende bandbreedtes berekenen. Dit gebeurt door middel van een in-house opgezette calculation engine, die uitgebreid getest is maar waarop in Q4 ook nog een interne modelvalidatie plaatsvindt. De doorlevering van de maandelijkse herijkte normallocaties en bandbreedtes aan de huidige Portfolio Management, Portfolio Risk Management en Reporting systemen is in Q3 afgerond, de business acceptance meetings hebben plaatsgevonden. Dit geldt ook voor de doorlevering van informatie over stortingen en onttrekkingen (informatiestroom 1b) en over af te dekken geprojecteerde uitkeringen (informatiestroom 1c), beide zijn afgerond en geaccepteerd door de relevante business units binnen VLK IM. Alle operationele veranderingen zijn in eigen beheer uitgevoerd, er worden geen extra taken uitbesteed als gevolg van WTP.

De nieuwe services worden STP (straight through processing) ingericht maar met de nodige controles. Naast een controle of de data ontvangen is, gaat VLK IM ook formatchecks en plausibiliteitschecks uitvoeren op de data. Deze plausibiliteitschecks worden in Q4 afgerond. Bevindingen vanuit deze checks worden teruggekoppeld naar de PUO. Alle proceswijzigingen binnen VLK IM zijn vastgelegd (AO/IC) en de Risk Control Self Assessment (RCSA) is afgerond. De outline van de ISAE 3402-controles zal in Q4 afgerond worden. Aangezien er geen SPR-processen live gaan per 1 januari 2025 zal VLK IM de ISAE-controles per 2026 in laten gaan.

Bijlage II: DORA

De Digital Operational Resilience Act (DORA) is begin 2023 in werking getreden. Vanaf 17 januari 2025 dienen financiële instellingen aan de DORA te voldoen. Deze nieuwe Europese verordening stelt uniforme eisen aan de beveiliging van informatie- en communicatietechnologie van ondernemingen die actief zijn in de financiële sector. Het doel van de DORA is om regelgeving op het gebied van ICT-veiligheid voor de sector te harmoniseren en de digitale weerbaarheid ervan verder te versterken. VLK en VLK IM dienen aan de DORA te voldoen.

VLK is nu al onderworpen aan regelgeving op het gebied van de beveiliging van ICT. Zoals in eerdere rapportages al is aangegeven voldoet VLK op basis van de eerder uitgevoerde gapanalyse op hoofdlijnen aan de DORA. Een projectorganisatie is ingericht om de aanwezige gaps te dichten.



Zoals we in ons vorige rapport hebben aangegeven, bestaat er in het kader van de DORA onduidelijkheid over de kwalificatie van asset managers als VLK IM. De vraag is of zij als ICT third-party service provider gekwalificeerd dienen te worden of niet. Hoewel hierover officieel door de ESA's nog geen uitspraak is gedaan heeft de DNB tijdens een DORA-seminar op 7 oktober jl. aangegeven dat financiële instellingen die onder toezicht staan, geen ICT third-party service providers zijn. De impact van deze kwalificatie is op onderdelen op het moment van schrijven van dit rapport nog onduidelijk, maar zal in ieder geval betekenen dat de contracten tussen VLK IM en haar cliënten niet DORA-compliant hoeven te worden gemaakt.

Desondanks onderkent VLK IM de behoefte van pensioenfondsen om meer inzicht te verkrijgen in de digital operational resilience van VLK en VLK IM en in de wijze waarop VLK-pensioenfondsen kan en gaat ondersteunen bij het nakomen van hun verplichtingen uit hoofde van de DORA. Om die reden zal VLK IM als onderdeel van haar DORA project komen met informatie over de wijze waarop VLK IM de volgende onderwerpen zal adresseren:

- Eventueel benodigde aanpassingen aan lopende contracten.
- Een overzicht van de reeds door VLK getroffen maatregelen op het gebied van information security en van de wijzigingen die VLK dienaangaande heeft doorgevoerd of zal doorvoeren n.a.v. DORA.
- Welke informatie VLK IM haar klanten zal verstrekken naar aanleiding van 'ICT-related incidents' zodat zij aan hun eventuele meldingsplicht kunnen voldoen.
- De wijze waarop VLK IM klanten kan faciliteren indien zij het verzoek krijgen een Threat Led Penetration Test uit te voeren.

Om haar cliënten over deze plannen en de voortgang van het VLK DORA-project te informeren, organiseert VLK IM deze periode 3 webinars. De eerste hiervan heeft plaatsgevonden op 24 september. Verdere seminars zullen worden georganiseerd begin december en in januari.

Status update Q3-2024:

Workstream ICT Management Framework:

- VLK's informatiebeveiligingsbeleid is aangepast en goedgekeurd. Dit beleid dient als basis voor de herziening van bestaand beleid, procedures en normen en het opstellen van nieuw beleid.
- De digital operational resilience strategy is goedgekeurd.
- De eerste 4 herziene security standards zijn aangepast.
- Review van VLK's business continuity management policy en data classification policy is onderhanden.
- Verwachting is dat de deadline gehaald zal worden.
- Belangrijkste uitdaging blijft het grote aantal vereisten. Dit kan ten koste gaan van de leesbaarheid, toepasbaarheid en duidelijkheid van het op te stellen beleid. Wij ondervangen dit door een gestructureerde en planmatige uitvoering van de door te voeren beleidswijzigingen.

Workstream Incident Management:

- Er is besloten om de bestaande incident management procedure niet aan te passen. Deze werkt goed.
- Er is een separate incident-meldprocedure ingericht, gericht op de melding van 'major incidents' aan toezichthouders. Deze procedure wordt momenteel getest.
- De voortgang is volgens plan.

Workstream Resilience Testing:

- VLK kent al een breed scala aan testen, variërend van vulnerability tests en penetration tests tot information security assessments bij third party serviceproviders.
- Waar nodig zijn deze tests aangepast om ze aan de eisen van de DORA te laten voldoen.
- Er zijn charters opgesteld voor VLK's IT-Security Red and Blue teams.
- De voorgang is volgens plan.

Workstream ICT Third Party Risk:

- Ook alle ICT third-party service providers die kritische of belangrijke functies ondersteunen zijn benaderd.
- Standaard contract addenda voor alle ICT third-party services zijn afgerond.
- Data vendoren die nog niet hebben gereageerd op ons verzoek aan te geven hoe zij willen inspelen op de DORA hebben een reminder ontvangen. Grotere partijen zoals Bloomberg hebben aangegeven zelf met addenda te komen.
- Het 'Beleid voor het gebruik van ICT-diensten ter ondersteuning van kritieke of belangrijke functies' is afgerond en zal in de vergadering van de Compliance & Operational Committee van 19 december worden goedgekeurd.
- Het verzamelen van data voor het Register of Information gaat gestaag voort. VLK's serviceprovider ISPNext heeft DORA-functionaliteit aan zijn contractmanagementapplicatie toegevoegd. Deze ondersteunt niet alleen de vastlegging van data maar ook de rapportages aan de toezichthouder. DNB heeft aangegeven dat het register waarschijnlijk in juni 2025 voor het eerst aangeleverd zal dienen te worden.
- VLK heeft geparticipeerd in de zogenaamde 'dry run' die door de ESA is georganiseerd. De feedback op onze input dienen wij nog te ontvangen.
- Grootste uitdaging: het aantal contracten dat moet worden gewijzigd en de hoeveelheid gegevens die moet worden geregistreerd. Bovendien verwacht VLK IM dat een groot deel van haar ICT third-party serviceproviders niet zonder meer akkoord zal gaan met de voorgestelde wijzigingen. Dit betekent dat VLK IM op dit punt naar verwachting de deadline niet zal halen. Van andere financiële instellingen krijgen we vergelijkbare signalen.

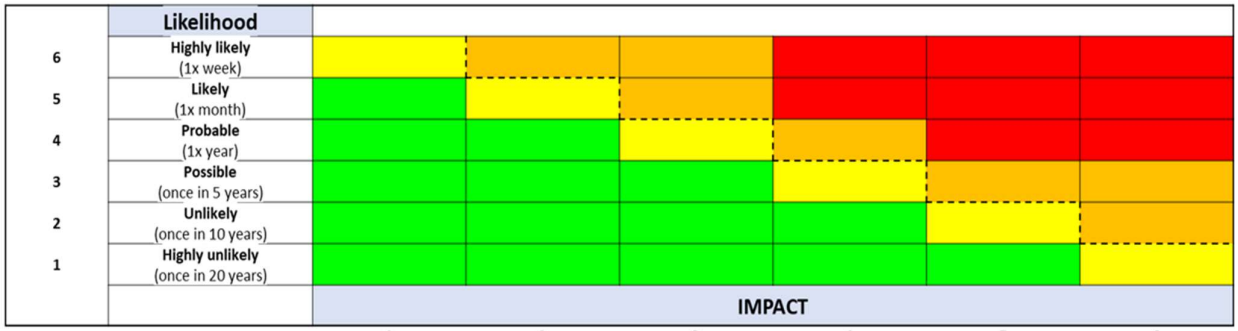
Gelet op de voortgang van het project verwacht VLK IM dat zij per 17 januari 2025 compliant zal zijn met uitzondering van de eisen die worden gesteld aan de contracten met ICT third-party service providers. Daar verwacht VLK IM nog steeds een langere doorlooptijd.

Bijlage III: Definities & beheersing risico taxonomie

Impactclassificatie

Deze bijlage toont de impactclassificatie zoals van toepassing op operationeel risicomanagement binnen VLK IM. Hiermee is inzichtelijk hoe de impact van incidenten wordt bepaald. Hierbij is professionele oordeelsvorming cruciaal, omdat het bepalen van de impact van incidenten complex kan zijn.

Vernieuwde heatmap per Q2 2024:



	1 Very Low	2 Low	3 Medium Low	4 Medium High	5 High	6 Very High
Financial impact	< EUR 25.000	EUR 25.000 - EUR 250.000	EUR 250.000 - EUR 1.000.000	EUR 1.000.000 - EUR 3.000.000	EUR 3.000.000 - EUR 5.000.000	> EUR 5.000.000
Client impact	No significant impact, only a few minor complaints	Limited impact, some negative feedback or minor inconveniences	Moderate impact for short-term (< 1 month)	Moderate impact for medium-term (> 1 month)	Significant impact for short-term (< 1 month)	Significant medium-term impact (> 1 month)
Reputational impact	None A few negative social media posts	Limited < 50 negative social media posts	Negative media attention for 1 or 2 days < 1,000 negative social media posts	Negative media attention over one week > 1,000 negative social media posts	Negative media attention lasting > 1 week Trust in VLK impaired International negative media attention	Negative media attention lasting > 1 month Trust in VLK significantly damaged International negative media attention
Regulatory Enforcement	No regulatory action	No regulatory action	Increased attention from regulator / meeting with regulator	Informal measure imposed by regulator (compliance briefing, warning letter)	Formal measure imposed by regulator (e.g. instruction / order subject to penalty)	(Very) heavy measure imposed by regulator (e.g. fine / restriction license)

Definitie risicocategorieën en risicomitigatie:

People risk:

Het risico van het overtreden van arbeidswetgeving, het verkeerd beheren van werknemersrelaties en het niet waarborgen van een veilige werkomgeving.

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	Subthema	
1.1 De organisatie-inrichting en/of overlegstructuren worden niet doelmatig ingericht.		De organisatie-inrichting en overlegstructuren zijn geformaliseerd en centraal beschikbaar gesteld voor de gehele VLK IM-organisatie. De opzet van beheersmaatregelen is getoetst met een inhoudelijke review van de centraal beschikbaar gestelde mandaten voor de overlegstructuren en onderliggende beleidsdocumenten. Daarnaast vindt herziening plaats wanneer nodig geacht, zodat overlegstructuren bij voortschrijdend inzicht effectief blijven.
1.2 De continuïteit voor sleutelfuncties wordt niet gewaarborgd.		• VLK IM-management en HR evalueren sleutelposities op jaarlijkse basis. • De succession planning is opgesteld voor functies vanaf een bepaalde senioriteit en een plan is opgesteld om interne doorgroei te stimuleren om de invulling van sleutelfuncties te waarborgen. • Periodieke monitoring vindt plaats op moeilijk vervulbare posities. Daarnaast worden HR-inspanningen verder geïntensiveerd om dit risico verder te mitigeren.
1.3 Nieuwe medewerkers voldoen niet aan vooraf gestelde kwaliteitseisen.		• Voor iedere nieuwe medewerker wordt de beheersmaatregel 'pre-employment-screening' uitgevoerd door HR. In de toetsingscyclus van beheersmaatregelen wordt deze maatregel getoetst door Group Compliance. • VLK IM-management checkt de competenties van medewerkers met een significante invloed op de VLK IM-bedrijfsresultaten en laat het profiel/achtergrond van de medewerker toetsen door de DNB.
1.4 De personeelsbezetting is kwalitatief onvoldoende.		• Lijnmanagers voeren gesprekken met medewerkers en formaliseren een persoonlijk plan waarin persoonlijke en professionele ontwikkel- en opleidingsbehoeften zijn opgenomen. Dit proces wordt gemonitord door HR. • Een ontwikkelplatform is beschikbaar om vaardigheden omtrent gedrag en expertise duurzaam en flexibel te ontwikkelen. De gedragsvaardigheden en expertise zijn inmiddels beschikbaar. • (Half)jaarlijkse evaluaties en monitoring vinden plaats, waarbij personeelsbezetting een terugkerend onderwerp is. HR toetst ook jaarlijks de uitvoering van het standaard en variabel beloningsbeleid door het senior management.

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	Subthema	
1.6 Voor de organisatie kunnen duurzaamheidsrisico's een negatieve invloed hebben op investeringen, investerings-performance en vice versa.		Momenteel wordt de formalisatie van ESG-beheersmaatregelen verder onderzocht en waar mogelijk uitgewerkt en geïmplementeerd. • Als onderdeel van het opstellen van het strategisch beleggingsbeleid stelt een klant haar eigen duurzaamheidsdoelen vast en VLK IM adviseert hierin. • VLK IM (a) vermijdt daarom voor haar klanten beleggingen in organisaties die betrokken zijn bij ernstige misstanden, (b) neemt materiële milieu (E), sociale (S) en governance (G); gezamenlijk 'ESG-factoren' overwegingen mee bij het nemen van investeringsbeslissingen (oftewel: ESG integratie), (c) tracht de invloed van VLK IM als belegger aan te wenden om bedrijven te stimuleren bepaalde misstanden aan te pakken en positieve verandering te bewerkstellingen, en (d) kiest waar mogelijk en met name in specifieke strategieën voor vermogensallocatie aan duurzame ondernemingen om meer positieve maatschappelijke impact helpen te realiseren. • Door deze aanpak beperkt VLK IM ook een belangrijk deel van de mogelijke duurzaamheidsrisico's. Duurzaamheidsrisico's raken echter ook duurzamere beleggingen. Een voorbeeld hiervan is dat ook een zonnepanelenproducent geraakt kan worden door de gevolgen van klimaatverandering zoals extreme weersverschijnselen. • Klanten formuleren steeds in toenemende mate een aantal duurzaamheidsrisico's inclusief een kwantitatieve risicobereidheid. VLK IM rapporteert over deze risico's en geeft daarbij ook een inschatting van de actuele kwaliteit van de maatstaven. Daarnaast is er sprake van bepaalde specifieke kwantitatieve targets, bijvoorbeeld op het gebied van carbon reductie, daarnaast worden er kwantitatieve stress testen gedaan. • Het identificeren van dergelijke risico's, het bepalen van de relevantie daarvan en de analyse ervan ligt in de eerste lijn bij de fiduciair managers. Zij worden hierbij ondersteund door specialisten vanuit het VLK Sustainability Centre. • Om de ontwikkelingen op het gebied van duurzaamheid te volgen, de strategie van de organisatie op het gebied van duurzaamheid te realiseren en er zorg voor te dragen dat wetgeving op het gebied van duurzaamheid tijdig wordt geïmplementeerd is binnen VLK een Sustainability Board opgezet. Deze wordt voorgezeten door de Chief Executive Officer (CEO) van VLK en daarnaast nemen deel, onder andere, de CEO van VLK IM en het Hoofd Financial Risk Management binnen VLK. • Ter ondersteuning van de Sustainability Board is daaronder een specifiek comité ingericht met een focus op VLK IM, het Sustainability Investment Committee. Op dit moment gaat er op het gebied van duurzaamheid veel aandacht naar het implementeren van (aanstaande) wet- en regelgeving en voldoen aan (aankomende) verwachtingen van toezichthouders, met name rondom de EU Sustainable Finance Disclosure Regulation (SFDR) en verwachtingen vanuit DNB ('Good Practice ESG-Risicobeheer Pensioenfondsen').
1.7 De organisatie besteedt onvoldoende aandacht aan toekomstige ontwikkelingen/klantwensen, waardoor klanttevredenheid daalt.		Dit wordt ondervangen door periodieke strategie-updates en interne managementbesprekingen waar dit onderwerp besproken wordt. Tijdens periodiek managementoverleg wordt besproken welke ontwikkelingen VLK ziet in de markt en waar VLK de klanttevredenheid verder kan verhogen. Dit is een continu proces.
1.8 De organisatie besteedt te veel aandacht aan nieuwe ontwikkelingen/ klantwensen, waardoor going concern activiteiten in het gedrang komen.		Voor haar klanten heeft VLK IM haar dienstenaanbod geformaliseerd in de 'dienstenmatrix'. Waar aanvullende of afwijkende dienstverlening gewenst is, worden de organisatie-brede haalbaarheid en het risicoprofiel hiervan geëvalueerd in het Product Approval & Review Process. Er vindt verdere specificatie van deze dienstenmatrix plaats om dit risico verder te mitigeren.

Physical security & safety:

Het risico van schade aan de fysieke activa van de organisatie of openbare activa waarvoor de organisatie aansprakelijk is, en (crimineel) letsel aan de werknemers of partners van de organisatie.

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	**Subthema**	
3.4 Facilities (ISAE 3402 over 2023 p. 88)	3.4.1 Physical security measures	• Dit betreffen de maatregelen m.b.t. fysieke toegangsbeveiliging tot de hardware bij het externe datacenter. • Geen bijzonderheden en/of onvolkomenheden.
3.4 Facilities (ISAE 3402 over 2023 p. 89)	3.4.2 Physical access	• Dit betreffen de maatregelen m.b.t. de toegangsrechten en autorisaties m.b.t. de datacenters. • Geen bijzonderheden en/of onvolkomenheden.

External fraud risk:

Frauduleuze activiteiten die worden gepleegd door personen of organisaties van buiten de eigen organisatie (d.w.z. een partij zonder directe relatie met de financiële instelling) zonder betrokkenheid van een werknemer of partner van de organisatie.

Uitgezonderd van External fraud risk:

- Wanneer het niet mogelijk is om de dader te bepalen, wordt het incident toegewezen aan 'first party fraud risk'.
- Gebeurtenissen gerelateerd aan datadiefstal zijn uitgesloten van externe fraude en worden toegewezen aan de risicocategorie 'Information security risk'.

Externe fraude komt bij VLK met name voor bij de private bank, als zijnde 'bank helpdesk' fraude. Hierbij monitort VLK continue betalingen en daarmee op zoek naar het voorkomen van externe fraude. Binnen VLK IM zijn de afgelopen periode geen gevallen van externe fraude bekend.

Internal fraud risk:

Fraude gepleegd of gepoogd door een interne partij (of partijen) tegen de organisatie, bijvoorbeeld een werknemer of gelieerde van de organisatie, inclusief gevallen waarbij een werknemer samenwerkt met externe partijen:

Uitgezonderd van Internal fraud risk:

- Diefstal of kwaadwillige beschadiging van fysieke activa wordt toegewezen aan de risicocategorie "Physical security & safety risk".
- Gebeurtenissen met betrekking tot datadiefstal worden toegewezen aan de risicocategorie "Information security risk".
- Terwijl belastingontduiking met betrekking tot de eigen belastingen van de organisatie wordt toegewezen aan Internal Fraud risk, wordt het risico van medeplichtigheid van organisaties bij het helpen van hun klanten of klanten bij belastingontduiking geclassificeerd onder Gedrag.

Het meest plausibele scenario voor interne fraude binnen VLK IM is managementfraude als gevolg van het doorbreken van functiescheiding (samenspanning), inadequate interne beheersing, gebrek aan ethiek en de hoge transactievolumes.

De risicobeheersing op interne fraude wordt met behulp van o.a. de volgende beheersmaatregelen gemitigeerd:

- Beleid en procedures m.b.t. Omkoping & Fraude, Gedragscode, Bankierseed, Pre-employment screening (PES).
- Toezicht, waarbij de Raad van Toezicht die toezicht houdt op de Raad van Bestuur. Toezicht van de Nederlandse Bank op de benoeming van bestuursleden.
- Aansprakelijkheidsverzekering
- Permanente educatie van medewerkers op het gebied van integriteit.
- Functiescheiding (Identity & access management, Chinese Walls)

Business continuity risk:

Falen van het business continuity management framework.

Uitgezonderd van Business continuity risk:

- Onbeschikbaarheid van fysieke activa wordt toegewezen aan Physical security & safety risk;
- Onbeschikbaarheid van systemen, inclusief telecommunicatie en nutsvoorzieningen, wordt toegewezen aan Technology risk;
- Onbeschikbaarheid van gegevens wordt toegewezen aan Datamanagement risk.

Risicospecificatie			Toelichting op de mate van beheersing
Risico	**Thema**	**Subthema**	
• Het Business Continuity Plan (BCP) niet periodiek wordt geoefend en/of aanbevelingen niet adequaat worden opgevolgd • Simulaties (cyber security attacks; pen testing) niet periodiek worden uitgevoerd en/of aanbevelingen niet adequaat worden opgevolgd	ICT availability and continuity risks	Inadequate capacity management	• Dit betreffen halfjaarlijkse risicoanalyses voor diverse DevOps afdelingen. • Geen bijzonderheden en/of onvolkomenheden.
		ICT-system failures	• De dagelijkse controle op de uitvoering van het back-up proces door IT Platformen & Security is effectief getoetst. Ook de toetsing van de effectiviteit van het 'restoration' proces van back-ups is effectief. • Geen bijzonderheden en/of onvolkomenheden.
		Inadequate ICT continuity and disaster recovery planning	• Het betreft beheersmaatregelen ten aanzien van het uitvoeren van (integrale) uitwijktesten en het valideren van de BCM-jaarkalender. • Geen bijzonderheden en/of onvolkomenheden.
		Disruptive and destructive cyber attacks	• Het betreft beheersmaatregelen ten aanzien van 'Policy Compliance', de activiteiten van het Red team en de wekelijkse beoordeling van (kritische) events rondom onder andere firewalls, (Azure) Active Directories, Databases en andere netwerkcomponenten. • Geen bijzonderheden en/of onvolkomenheden.

Transaction processing & (change) execution risk:

Het niet verwerken, beheren en uitvoeren van transacties en/of andere processen (zoals veranderprogramma's) op een correcte en/of passende manier.

Uitgezonderd van transaction processing & (Change) execution risk:

- Uitvoeringsfouten, bijvoorbeeld het niet nauwkeurig vastleggen van zakelijke transacties in het grootboek, worden toegewezen aan Transaction Processing and (change) Execution risk, in plaats van Statutory Reporting and Tax risk.
- Risico-evenementen met betrekking tot gegevensverzameling worden toegewezen aan Transaction Processing and (change) Execution risk, tenzij ze direct verband houden met gegevensbeheer, in welk geval ze worden toegewezen aan Data Management risk.

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	**Subthema**	
2.2 Account Management (ISAE 3402 over 2023 p. 59 t/m 61)	Intake, wijziging en exit van klanten, fund setup en klachtafhandeling vinden onjuist, niet tijdig en/of onvolledig plaats.	Geen bijzonderheden en/of onvolkomenheden.
2.3 Issuance and Redemption of shares and participations (ISAE 3402 over 2023 p. 62)	Fund orders worden onjuist, niet tijdig en/of onvolledig verwerkt.	Geen bijzonderheden en/of onvolkomenheden.
2.4 Portfolio management	Client Portfolio's worden niet conform richtlijnen gemanaged.	Geen bijzonderheden en/of onvolkomenheden voor de institutionele doelgroep.

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	Subthema	
(ISAE 3402 over 2023 p. 63 t/m 65)		
2.5 Portfolio Risk Management (PRM) (ISAE 3402 over 2023 p. 66 en 67)	Monitoring van risk exposures, investment restricties en uitbestede dienstverlening voor client portfolio's voldoet niet aan de richtlijnen.	Geen bijzonderheden en/of onvolkomenheden.
2.6 Trade Execution (ISAE 3402 over 2023 p. 68)	3.3 Transacties worden niet tijdig en/of correct uitgevoerd.	Geen bijzonderheden en/of onvolkomenheden.
2.7 Trade Processing and Reconciliation (ISAE 3402 over 2023 p. 69 t/m 73)	3.3 Transacties worden niet juist, tijdig en/of volledig verwerkt of gereconcilieerd.	Ten aanzien van de beheersmaatregel is er een bevinding geconstateerd welke geen materiële impact heeft op de daarbij behorende processen en controle doelstellingen. Relevante acties zijn inmiddels opgevolgd om de bevinding in de toekomst te voorkomen. Zie voor een uitgebreide toelichting het ISAE-rapport over 2023.
2.9 Accounting and Reporting (ISAE 3402 over 2023 p. 75 t/m 78)	Klantrapportages en naleving van fee afspraken worden juist tijdig en volledig uitgevoerd.	Geen bijzonderheden en/of onvolkomenheden.
2.10 Error Handling (ISAE 3402 over 2023 p. 79)	Operationele incidenten worden niet adequaat opgevolgd waardoor voor klanten mogelijk materiële of reputatieschade ontstaat.	Geen bijzonderheden en/of onvolkomenheden.
De kwaliteit van de processen onvoldoende is en/of procesinrichting is te complex waardoor incidenten optreden		Het management van VLK IM coördineert de continue aanscherping van het interne beheersingsraamwerk met de verschillende business teams met het doel proceskwaliteit en procesinrichting verder te versterken. Dit komt terug in het jaarplan dat NFRM en Compliance onder andere voor VLK IM hebben geformuleerd. NFRM merkt op dat huidige processen nog verder kunnen worden geautomatiseerd, waarmee risico's verder kunnen worden verlaagd. Dit vindt plaats in samenspraak tussen de VLK IM business en IT middels het doorgeven van prioriteiten en het doorvoeren van wijzigingen binnen de betreffende processen.
Kritische modellen worden niet tijdig of niet adequaat gevalideerd		• VLK IM heeft een Model Validation Committee dat toeziet op validatie van kritische modellen conform het beleid voor modelvalidatie. • Voor de toepassing van End User Computing ziet NFRM i.s.m. Model Risk toe op de naleving van het EUC-beleid. Hierbij is het afgelopen jaar o.a. het model landschap binnen VLK IM geïnventariseerd.
Risk & Control Self-Assessments (RCSA's) vinden niet periodiek plaats.		NFRM coördineert jaarlijks een centrale zelfbeoordeling met het VLK IM-management en op verzoek ook voor waardeketen specifieke thema's en/of business units. Hierdoor vinden frequente risicoanalyses en opvolging plaats door de gehele VLK IM-organisatie heen. Een onderdeel hiervan zijn de zogeheten 'Value Chain Risk and Control Self-Assessments'. Hierbij wordt niet enkel naar een individueel proces gekeken, maar naar de

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	Subthema	
		gehele end-to-end keten. Hierdoor wordt de onderlinge afstemming van belangrijke, individuele bedrijfsprocessen meegenomen in de zelfbeoordelingen.
Risk awareness sessies vinden niet periodiek plaats		NFRM brengt risicobewustzijn ter sprake in sub-management en groepsoverleggen om zo een risicobewuste cultuur te stimuleren.
Aanbevelingen uit interne audits worden niet tijdig en/of adequaat opgevolgd.		NFRM monitort opvolging van aanbeveling van interne audits voor heel VLK IM. De inhoudelijke beoordeling van de opvolging ligt bij de VLK Internal Audit functie.

Technology risk:

Het risico verbonden aan het falen of uitvallen van systemen, inclusief hardware, software en netwerken.

Uitzonderingen van technology risk:

- Misbruik van technologie om interne fraude te faciliteren wordt toegewezen aan Internal Fraud risk.

Risicospecificatie			Toelichting op de mate van beheersing
Risico	Thema	Subthema	
• Het Business Continuity Plan (BCP) niet periodiek wordt geoefend en/of aanbevelingen niet adequaat worden opgevolgd** • Simulaties (cyber security attacks; pen testing) niet periodiek worden uitgevoerd en/of aanbevelingen niet adequaat worden opgevolgd	ICT availability and continuity risks	Inadequate capacity management	• Dit betreffen halfjaarlijkse risicoanalyses voor diverse DevOps afdelingen. • Geen bijzonderheden en/of onvolkomenheden.
		ICT-system failures	• De dagelijkse controle op de uitvoering van het back-up proces door IT Platformen & Security is effectief getoetst. Ook de toetsing van de effectiviteit van het 'restoration' proces van back-ups is effectief. • Geen bijzonderheden en/of onvolkomenheden.
		Inadequate ICT continuity and disaster recovery planning	• Het betreft beheersmaatregelen ten aanzien van het uitvoeren van (integrale) uitwijktesten en het valideren van de BCM-jaarkalender. • Geen bijzonderheden en/of onvolkomenheden.
		Disruptive and destructive cyber attacks	• Het betreft beheersmaatregelen ten aanzien van 'Policy Compliance', de activiteiten van het Red team en de wekelijkse beoordeling van (kritische) events rondom onder andere firewalls, (Azure) Active Directories, Databases en andere netwerkcomponenten. • Geen bijzonderheden en/of onvolkomenheden.

Third party risk:

Het risico van het niet adequaat beheren van relaties en risico's van derden, bijvoorbeeld door geen redelijke stappen te ondernemen om aanvullende operationele risico's te identificeren en te beperken die voortvloeien uit het uitbesteden van diensten en functies.

De volgende items worden niet beschouwd als risico van derden, om overlap tussen categorieën te voorkomen:

- Contractuele kwesties van derden (toegewezen aan Legal)
- Niet-presteren van derden, bijvoorbeeld het niet nakomen van contractuele verplichtingen, tekortkomingen van derden en faillissement, wordt beschouwd als een oorzaak van een risico-evenement.
- Geschillenrisico met derden wordt beschouwd als bedrijfsrisico.
- Concentratierisico wordt niet behandeld als een op zichzelf staand risico-event, maar wordt in plaats daarvan beschouwd als een maatstaf die wordt gebruikt voor het beheren van risico's van derden.
- Risico-events gerelateerd aan systeemfouten van derden worden toegewezen aan technology risk.

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	**Subthema**	
2.5.3 Activiteiten uitgevoerd door derde partijen (buiten de VLK IM-organisatie) worden ontoereikend beheerst** (ISAE 3402 over 2023 p. 67)	Door VLK IM risico-gebaseerde uitbestede dienstverlening aan derde partijen wordt niet adequaat en/of tijdig gemonitord.	• Geen bijzonderheden en/of onvolkomenheden. • Gedurende Q3 2024 hebben zich geen materiële incidenten rond serviceproviders voorgedaan. • Gedurende Q3 2024 heeft VLK IM de monitoring van de uitbestedingspartijen in overeenstemming met de opgenomen elementen uitgevoerd.

Information security (including cyber) risk:

Het risico van informatiebeveiligingsincidenten, inclusief het verlies, diefstal of misbruik van gegevens/informatie; dit omvat alle soorten gegevens, bijvoorbeeld klantgegevens, werknemersgegevens en de eigen gegevens van de organisatie, en kan het niet naleven van regels met betrekking tot informatiebeveiliging omvatten.

Risicospecificatie			Toelichting op de mate van beheersing
Risico	**Thema**	**Subthema**	
• Het Business Continuity Plan (BCP) niet periodiek wordt geoefend en/of aanbevelingen niet adequaat worden opgevolgd** • Simulaties (cyber security attacks; pen testing) niet periodiek worden uitgevoerd en/of aanbevelingen niet adequaat worden opgevolgd	ICT availability and continuity risks	Inadequate capacity management	• Dit betreffen halfjaarlijkse risicoanalyses voor diverse DevOps afdelingen. • Geen bijzonderheden en/of onvolkomenheden.
		ICT-system failures	• De dagelijkse controle op de uitvoering van het back-up proces door IT Platformen & Security is effectief getoetst. Ook de toetsing van de effectiviteit van het 'restoration' proces van back-ups is effectief. • Geen bijzonderheden en/of onvolkomenheden.
		Inadequate ICT continuity and disaster recovery planning	• Het betreft beheersmaatregelen ten aanzien van het uitvoeren van (integrale) uitwijktesten en het valideren van de BCM-jaarkalender. • Geen bijzonderheden en/of onvolkomenheden.
		Disruptive and destructive cyber attacks	• Het betreft beheersmaatregelen ten aanzien van 'Policy Compliance', de activiteiten van het Red team en de wekelijkse beoordeling van (kritische) events rondom onder andere firewalls, (Azure) Active Directories, Databases en andere netwerkcomponenten. • Geen bijzonderheden en/of onvolkomenheden.
• Informatiesystemen en -procedures niet goed ingeregeld zijn waardoor onveilig	ICT-security risks	Cyber-attacks and other external ICT based attacks	• Hiervoor geldt hetzelfde als verwoord bij het subthema 'disruptive and destructive cyber attacks'. • Geen bijzonderheden en/of onvolkomenheden.

Risicospecificatie			Toelichting op de mate van beheersing
Risico	**Thema**	**Subthema**	
gebruik van informatie en/of onbetrouwbaar datagebruik kan plaatsvinden** • Kritische bedrijfsprocessen niet beschermd zijn tegen grote fouten en uitval van informatiesystemen** • De toegang tot kritieke systemen en applicaties niet beperkt is tot de daartoe bevoegden** • IT-awareness trainingen niet periodiek plaats vinden		Inadequate internal ICT-security	• Deze beheersmaatregelen hebben betrekking op het toekennen en intrekken van autorisaties in het geval van personeelsmutaties, de creatie van niet persoonlijke useraccounts, de 'password policy', het beoordelen van de toegekende autorisaties van kritische informatiesystemen en het gebruik van de 'corporate password vault'. Ook wordt gekeken naar autorisaties die buiten het reguliere proces om worden toegekend. • Geen bijzonderheden en/of onvolkomenheden.
		Inadequate physical ICT-security	• Deze beheersmaatregelen hebben betrekking op het periodieke serviceoverleg met de leverancier van het externe datacenter en de halfjaarlijkse review op verstrekte toegangsrechten voor IT-ruimtes welke VLK in gebruik heeft. • Geen bijzonderheden en/of onvolkomenheden.
• Functionele wijzigingen in applicaties op onjuiste wijze worden geïmplementeerd en gedocumenteerd** • IT-incidenten niet tijdig en juist worden gecorrigeerd en gecommuniceerd**	ICT-change risks	Inadequate controls over ICT-system changes and ICT-development	• De beheersmaatregelen hebben betrekking op het (Agile) change managementproces wat als doel heeft om wijzigingen op een gestandaardiseerde en gecontroleerde wijze te implementeren, met een minimale kans op verstoringen. • Geen bijzonderheden en/of onvolkomenheden.
		Inadequate ICT architecture	• Dit betreffen halfjaarlijkse risicoanalyses voor diverse DevOps afdelingen. • Geen bijzonderheden en/of onvolkomenheden.
		Inadequate lifecycle and patch management	• Dit betreffen halfjaarlijkse risicoanalyses voor diverse DevOps afdelingen. • Geen bijzonderheden en/of onvolkomenheden.
End user computing toepassingen niet tijdig of niet adequaat worden gecontroleerd	ICT-data integrity risks	Dysfunctional ICT-data processing or handling	• Dit betreffen halfjaarlijkse risicoanalyses voor diverse afdelingen. • Geen bijzonderheden en/of onvolkomenheden.
		III designed data validation controls in ICT-systems	
		Ill controlled data changes in the production ICT-systems.	
		Ill designed and/or managed data architecture, data flows, data models or data dictionaries	• De beheersmaatregelen zien toe op de correcte en tijdige uitvoering van batches c.q. interfaces en op de adequate opvolging van eventuele afwijkingen en/of verstoringen. • Geen bijzonderheden en/of onvolkomenheden.

Cyber security: De risico's en beheersmaatregelen rondom cybercriminaliteit worden binnen VLK centraal gemonitord. Ieder kwartaal rapporteert het CISO over deze risico's en beheersmaatregelen aan het Compliance en Operational Risk Committee. De rapportage is gecategoriseerd op basis van de onderdelen 'People', 'Process' en 'Technology' en omvat verschillende indicatoren ten aanzien van informatiebeveiliging en (cyber) security, verdeeld over verscheidene risicocategorieën. De volgende onderdelen uit de CISO-rapportage over Q3-2024 zijn noemenswaardig:

- In Q3-2024 hebben zich geen kritische security incidenten voorgedaan welke een significante impact hebben gehad op de operationele processen van VLK IM.

- Het aantal afgeronde (awareness) sessies rondom cyber security en/of informatiebeveiliging ligt gelijk aan voorgaande kwartaal. In totaal zijn er het afgelopen kwartaal tien verschillende sessies en/of campagnes gehouden.
- De wachtwoordsterke van user ID's in zowel de Productie-omgeving als de Acceptatie-omgeving welke met de maandelijkse kraakexercitie wordt gemeten, blijft onverminderd hoog. Het aantal gekraakte user ID's (van reguliere user accounts) in de Productie-omgeving ligt in het derde kwartaal wel hoger dan in het tweede kwartaal van 2024 maar dit is te verklaren door het zeer grote aantal in dienst getreden medewerkers per september 2024.
- De 'Password Identification Tool' (PIT) - welke ontwikkeld is door het Red team - identificeert mogelijke 'plaintext passwords' op servers. In het tweede kwartaal van 2024 lag het totale aantal geïdentificeerde potentiële 'plaintext passwords' significant hoger ligt dan in het eerste kwartaal van 2024. In het derde kwartaal van 2024 is ruim 95 van de geïdentificeerde potentiële 'plaintext passwords' opgevolgd voor de verantwoordelijke teams.
- Het totaal uitgevoerde penetratietesten in het derde kwartaal ligt hoger dan in het tweede kwartaal van 2024.
- Ieder kwartaal wordt een aantal technologieën gekozen waarvoor de System Hardening (Policy Compliance) verbeterd dient te worden door de verantwoordelijke beheerteams in overleg met IT Security. De technologieën die voor Q3 2024 gekozen zijn hebben een sterke verbetering laten zien, maar voldoen nog niet volledig aan de door VLK gestelde eisen zoals vastgelegd in de desbetreffende Security Standard. Daarnaast is de onderliggende Roadmap voor Policy Compliance herzien en zijn de prioriteiten voor de komende kwartalen bepaald in overleg met Management.
- Het aantal kwetsbaarheden in onderdelen van de IT-infrastructuur is stabiel en laat dit kwartaal een gelijkmatige trend zien. Gelijk aan de eerdere kwartalen in 2024 vallen alle beheerteams nog steeds in de laagste categorie (Low).
- Het totaal aantal afgegeven excepties ten aanzien van de geldende Security Standards is ten opzichte van het afgelopen kwartaal met één exceptie afgenomen.

Statutory reporting & tax risk:

Het risico van het niet voldoen aan wettelijke rapportage- en belastingbetalings-/aangifteverplichtingen.

Uitzonderingen op statutory reporting & tax risk:

- Statutory reporting omvat alle externe rapportages die de organisatie verplicht is uit te voeren, bijvoorbeeld regelgevende rapportage, financiële rapportage.
- Omvat alle gebeurtenissen gerelateerd aan management accounting.
- Omvat rapportagefouten in verband met het gebruik van foutieve gegevens; let op dat hier de gegevensfout de oorzaak is van een risico-gebeurtenis en daarom niet als een Data management risico-gebeurtenis op zich wordt geclassificeerd.
- Risico's met betrekking tot het slecht beheren van regelgevende interactie, op voorwaarde dat deze niet zijn gebaseerd op juridische uitvoeringsfouten, in welk geval het risico-gebeurtenis wordt toegewezen aan Legal risico.
- Belastingontwijking/-ontduiking door de organisatie en boekhoudfraude worden toegewezen aan Internal Fraud risk.
- Uitvoeringsfouten, bijvoorbeeld fouten die voortkomen uit het niet nauwkeurig vastleggen van bedrijfstransacties in het grootboek, worden toegewezen aan transaction processing & (change) execution risk.

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	Subthema	
2.5.3 Activiteiten uitgevoerd door VLK voor klanten die regulatory reporting diensten afnemen worden ontoereikend beheerst** (ISAE 3402 over 2023 p. 78)	Door VLK IM worden regulatory rapportages geleverd aan klanten (J402 en Solvency II rapporten)	• Geen bijzonderheden en/of onvolkomenheden.

Data management risk:

Het risico van het niet goed beheren en onderhouden van gegevens, inclusief alle soorten gegevens, bijvoorbeeld klantgegevens, werknemersgegevens en de eigen gegevens van de organisatie.

Uitzonderdingen op data management risk:

- De ORX-referentietaxonomie definieert data management om risico-events in een post-capture-fase van de gegevenslevenscyclus te dekken. Risico-events die verband houden met het vastleggen van gegevens worden in plaats daarvan toegewezen aan transactieverwerking en -uitvoering. Als een foutief data managementproces echter de oorzaak is van onnauwkeurige gegevensrecords, wordt het risico-item geclassificeerd onder slechte gegevenskwaliteit, binnen data management risk.
- Risico-events met betrekking tot foutieve gegevens die worden gebruikt bij het opstellen van interne rapporten, worden toegewezen aan Statutory reporting & Tax risk.
- Risico-events met betrekking tot gegevensbescherming worden toegewezen aan information security risk.

Risicospecificatie		Toelichting op de mate van beheersing
Risicothema	**Subthema**	
2.8 Data Management (ISAE 3402 over 2023 p. 74 en 75)	3.4 Static Data van instrumenten wordt niet juist, tijdig en volledig geüpdatet.	Geen bijzonderheden en/of onvolkomenheden.

Integrity-/Compliance risk:

Compliance-risico's zijn gedefinieerd als het risico dat VLK:

I) Er niet in slaagt regelgeving na te leven die van toepassing is op VLK en haar activiteiten en/ of

II) Activiteiten onderneemt die verboden zijn of nalaat te ondernemen die verplicht zijn onder de toepasselijke regelgeving, gezamenlijk 'compliance-risico's'.

Compliance-risico's omvatten voor dit rapport de volgende integriteitsrisico's bepaald op basis van de Systematische Integriteitsrisicoanalyse (SIRA)-classificatie van DNB: integriteit van persoonsgegevens, anti-financiële criminaliteit (waaronder anti-witwassen, sanctieregelgeving en belastingintegriteit van cliënten), marktgedrag (marktmisbruik), belangenverstrengeling en integriteit van werknemers.

De compliance-risico's die van toepassing zijn op VLK IM, worden door Compliance doorlopend beoordeeld aan de hand van een specifieke risicobeoordeling en aan het VLK IM-bestuur voorgelegd. Compliance rapporteert vervolgens op basis van de risicobeoordeling en de bijstellingen die daarin gedurende een kwartaal zijn gemaakt, als gevolg van bijvoorbeeld afronden van acties, geconstateerde incidenten, uitkomsten van monitoring op beheersmaatregelen en deep-dives of het wijzigen van toepasselijke regelgeving.

Risicospecificatie			Toelichting op de mate van beheersing
Risico	**Thema**	**Subthema**	
Algemeen	Anti-Financial Crime	Bribery & Corruption	Deze onderwerpen worden op VLK-groepsniveau geadresseerd. Er zijn beleidsdocumenten opgesteld en ingevoerd (waaronder een Anti-Bribery and Corruption Policy, een Gift & Entertainment Policy en een Client Tax Integrity Policy). Deze beleidsdocumenten zijn intern beschikbaar gemaakt voor medewerkers en (verplichte) trainingen (waaronder door middel van e-learnings) worden gegeven.
		Client Tax Integrity	
Account Management proces		Money Laundering & Terrorism Financing	Compliance heeft voor dit onderwerp beleidsdocumenten en specifieke instructiedocumenten opgesteld en er zijn beheersmaatregelen geïmplementeerd. De CDD gerelateerde werkzaamheden worden binnen Van Lanschot Kempen centraal uitgevoerd door de afdeling Client Administration & Monitoring , ook voor VLK IM. De uitgevoerde beheersmaatregelen op dit gebied zijn dit kwartaal als effectief getest.

Risicospecificatie			Toelichting op de mate van beheersing
Risico	Thema	Subthema	
			Eind september bleek de gestelde limiet voor het aantal niet tijdig afgeronde CDD-dossierreviews te zijn overschreden, in totaal waren 6 van de 32 geplande beoordelingen van VLK IM dossiers niet bijtijds afgerond. Dit is in oktober alsnog verholpen.
Account Management proces; Portfolio Investment proces		Sanctions	Voor dit onderwerp is een beleidsdocument opgesteld en zijn diverse beheersmaatregelen ingericht. De uitgevoerde beheersmaatregelen met betrekking tot de processen gericht op sanctiescreening zijn dit kwartaal als effectief getest.
Account Management proces; Portfolio Investment proces	Conduct of Business	Conflict of Interest	Voor dit onderwerp zijn beleidsdocumenten opgesteld en geïmplementeerd. Het identificeren en adresseren van belangenconflicten is een onderdeel van ingerichte governance, zoals bijvoorbeeld het Product Approval and Review proces. Belangenconflicten worden bijgehouden in een register dat periodiek door senior management wordt besproken. VLK IM heeft op de website een samenvatting van het beleid gepubliceerd.
Algemeen		Employee Conduct and Integrity	Deze onderwerpen worden op VLK-niveau geadresseerd. Voor deze risico's zijn beleidsdocumenten opgesteld, zoals een Code of Conduct, regeling persoonlijke transacties en regeling nevenfuncties. In het aannamebeleid zijn maatregelen ten aanzien van screening ingericht. Medewerkers moeten bij aanvang en gedurende hun dienstverband verplicht trainingen volgen, onder andere in de vorm van e-learnings. Bij indiensttreding wordt eveneens de Bankierseed afgenomen. Er zijn beheersmaatregelen opgesteld voor personeelstransacties en in de vorm van beleid op het gebied van marktmisbruik en een insiderregeling. Per categorie medewerkers van VLK IM gelden handel- en transactierestricties, ter mitigatie van potentieel marktmisbruik en belangenconflicten door privé beleggingstransacties. Een beheersmaatregel met betrekking tot pre-employment screening is dit kwartaal als ineffectief getest. In twee gevallen bleek een deel van de screening niet afgerond voor de eerste werkdag. Acties ter verbetering worden in overleg tussen Internal Control en de proces-eigenaar bepaald.
Portfolio Investment proces	Conduct of Business	Market Conduct	Voor dit onderwerp zijn beleidsdocumenten opgesteld en geïmplementeerd, waaronder een Market Conduct Policy. Met betrekking tot monitoring op marktmisbruik zijn systemen in gebruik om orders en transacties te analyseren en waar nodig aan toezichthouders te rapporteren.
		Market Infra-structure and Investor Protection	Er zijn beleidsdocumenten opgesteld en ingevoerd. De gedurende dit kwartaal geteste maatregelen beslaan meerdere onderwerpen, waaronder 'Disclosure of Significant Positions', en 'Securities and Derivatives Processing'. De dit kwartaal geteste maatregelen zijn allen effectief bevonden.
Algemeen	Personal Data Integrity		Deze risico's worden op VLK-niveau geadresseerd. Voor deze risico's zijn beleidsdocumenten opgesteld en beschikbaar gesteld voor medewerkers. VLK heeft een Privacy Officer aangesteld, die toezicht houdt op naleving van de vereisten uit de AVG. De Privacy Officer rapporteert hierover aan de Privacy Committee van VLK. Gedurende dit kwartaal zijn ten aanzien van VLK IM geen tekortkomingen geconstateerd.

Legal risk:

Het risico samenhangend met (veranderingen in en naleving van) wet- en regelgeving, het mogelijk bedreigd worden van haar rechtspositie, met inbegrip van de mogelijkheid dat contractuele bepalingen niet afdwingbaar of niet correct gedocumenteerd zijn waardoor VLK IM en/of haar cliënten reputatie- en of vermogensschade kunnen oplopen.

Risicothema	Toelichting op de mate van beheersing
Relevante wijzigingen in wet- en regelgeving niet, of niet tijdig, worden gesignaleerd	De afdeling Legal signaleert relevante wijzigingen in Nederlandse en EU wet- en regelgeving en informeert de organisatie daarover. Op kwartaalbasis wordt het overzicht met relevante wijzigingen in wet- en regelgeving geactualiseerd en aan relevante stakeholders gezonden.
Relevante (wijzigingen in) wet- en regelgeving niet wordt nageleefd	Bij implementatie van relevante (wijzigingen in) wet- en regelgeving zijn Legal en Compliance nauw betrokken. De afdeling Compliance heeft een monitoringsprogramma om doorlopende compliance aan wet- en regelgeving met regelmaat te toetsen.
Afspraken (of wijzigingen daarin) niet contractueel worden vastgelegd	Voor deze onderdelen heeft NFRM geconstateerd dat processen zijn ingericht en beheersmaatregelen bestaan in de organisatie. NFRM evalueert doorlopend in welke mate verdere formalisering van processen en beheersmaatregelen plaats kan vinden teneinde het netto risico verder te verlagen. De afdeling Legal ondersteunt de commerciële activiteiten en fiduciair beheeractiviteiten. Daarnaast hebben geen noemenswaardige incidenten plaatsgevonden. Ten aanzien van klachten zijn processen geïntegreerd waardoor, indien klachten worden ontvangen door VLK IM, deze centraal worden geregistreerd en opgevolgd en er centraal over wordt gerapporteerd.
Juridische risico's niet adequaat afgedekt worden in contracten	
Contracten (of wijzigingen daarin) niet worden nagekomen	
Klachten niet gemeld worden bij de afdeling Kwaliteit & Service (klachtenmanagement)	
Klachten niet conform de klachtenprocedure worden afgehandeld	

Bijlage IV: Beleidsdocumenten

Deze bijlage toont de voor VLK IM relevante beleidsdocumenten gegroepeerd per onderwerp.

Onderwerp	Beleidsdocumenten
Duurzaamheidsbeleid en HR	VLK Beloningsbeleid
	VLK Variabel Beloningsbeleid
	VLK Beleid Screening Medewerkers
	VLK IM engagement policy & stewardship beleid
	VLK IM Proxy Stembeleid
	VLK IM Klimaatbeleid
Risicomanagement	VLK IM Risk Management Beleid
	VLK IM Counterparty Risk Beleid
	VLK IM Market Risk Beleid
	VLK IM Liquidity Risk Beleid
	VLK IM Model Governance framework
	VLK IM Swing Price Beleid
	VLK IM Trading Principles
	VLK (Group Risk) ORM Framework
	VLK IM Incident & Action Policy
Uitbestedingsbeleid	VLK Outsourcing Policy
	VLK Centraal Inkoopbeleid
	VLK Regeling Business Partner Due Diligence
IT	VLK (Groep Risk) Informatiebeveiligingsbeleid
	VLK (Group Risk) Business Continuity beleid
	VLK (Group Risk) Guidelines End User Computing
	VLK (Group Risk) Standard process, application and data classification policy
	VLK (CISO) Security Standard - Access Control
	VLK (CISO) Security Standard - Audit Log Management
	VLK (CISO) Security Standard - Authentication mechanism & Password restrictions
	VLK (CISO) Security Standard - Backup & Restoration
	VLK (CISO) Security Standard - Cryptography
	VLK (CISO) Security Standard - Cyber Security Incidents
	VLK (CISO) Security Standard - Development, Testing, Acceptance and Production Environments
	VLK (CISO) Security Standard - Endpoint Protection
	VLK (CISO) Security Standard - Mobile Device Management
	VLK (CISO) Security Standard - Network Security
	VLK (CISO) Security Standard - Penetration Testing
	VLK (CISO) Security Standard - Physical Access Control for IT equipment
	VLK (CISO) Security Standard - Remote Access 3rd-parties
	VLK (CISO) Security Standard - Securing email
	VLK (CISO) Security Standard - System hardening
	VLK (CISO) Security Standard - Vulnerability Management
Juridisch	VLK Overzicht relevante wet- en regelgeving
	VLK IM Standaard Fiduciair Beheer overeenkomsten (NL- & VK-versie)
	VLK IM Klachtenprocedure(s)

Bijlage V: Overzicht Onderuitbestedingen VLK IM

Deze bijlage toont de generieke uitbestedingen naar type uitbesteding met daarbij een korte omschrijving van de uitbesteding. Dit overzicht wordt periodiek geüpdatet.

Naam serviceprovider	Naam toepassing indien deze afwijkt van naam service provider	Type Uitbesteding	Korte omschrijving uitbesteding
Broadridge Financial Solutions, Ltd*	Broadridge Revport	Software as a Service (SaaS)	Facturatie tool
Canoe Software Inc.	Canoe	Software as a Service (SaaS)	Automatisering tool voor verzamelen van alternatieve investeringsdocumentatie
S&P Global Limited	iLevel	Software as a Service (SaaS)	Portfolio monitoring tool voor portefeuilles met alternatieve investeringen
FactSet UK Limited		Software as a Service (SaaS)	FactSet levert aan VLK IM een breed pakket aan functionaliteit: a. downloaden van financiële data van bedrijven b. opslaan van research c. koersinformatie d. broker reviews & research e. nieuwsdiensten f. performance measurement benchmarking (UK klanten) In dit kader worden via FactSet ook geüploade data verrijkt
Fundapps Ltd		Software as a Service (SaaS)	Shareholder disclosure tool
Institutional Shareholder Services Europe SA/NV		Software as a Service (SaaS)	Analyse tool op gebied van socially responsible investments
IQ/EQ		Business Process Outsourcing (BPO)	Data collectie en management ten behoeve van Alternatieve Investment Solutions mandaten (private markets)
TriOptima AB	TriResolve Margin	Software as a Service (SaaS)	Reconciliatie & collateral management tool
Microsoft BV	Microsoft Dynamics	Software as a Service (SaaS)	CRM-tool incl. procesondersteuning middels workflows
Diligence Vault Corp		Software as a Service (SaaS)	Portal voor informatie-uitwisseling rondom manager due dilligence . Data dient als input voor client reporting
Van Lanschot Kempen N.V.		Business Process Outsourcing (BPO)	Van Lanschot Kempen N.V. levert ondersteunende diensten aan Van Lanschot Kempen Investment Management N.V. op het gebied van HR, IT-infra, - security and - development, Legal, Finance & Control etc.
Kritische & belangrijke service providers van Van Lanschot Kempen N.V. die een bijdrage leveren aan de dienstverlening van Van Lanschot Kempen Investment Management N.V.			
Microsoft BV	MS 365	Software as a Service (SaaS)	Werkplekautomatisering
Microsoft BV	Azure	Software as a Service (SaaS)	Hosting services en ontwikkelplatform
Interconnect services B.V.		Data Center Services	Colocatie datacenter. Hier host VLK haar on premise draaiende software
* Sinds een paar jaar hoeft alleen melding plaats te vinden van kritische en belangrijke uitbestedingen. Melding van Broadridge heeft voordien plaatsgevonden.			

Bijlage VI: Informatiebeveiligingsstandaarden

Onderstaande tabel geeft weer hoe VLK IM de informatiebeveiligingsonderwerpen zoals voorgeschreven door enerzijds DNB (kolommen) en anderzijds de Europese Bankautoriteit (EBA, regels) combineert. Hierdoor geeft VLK IM invulling aan de eisen zoals voorgeschreven door beide toezichthouders. De tabel geeft de aansluiting weer tussen de (sub)onderwerpen vanuit beide perspectieven.

		DNB topics																			
		1. Define an information security plan	2. Define the information architecture	3. Determine technological direction	4. Assess and manage (IT) risks	5. Information Security Organization	6. Data and system ownership	7. Manage segregation of duties	8. Manage IT human resources	9. Ensure operations and use	10. Change Management	11. Continuity Management	12. Manage data	13. Configuration Management	14. Manage third party and supplier services	15. Incident Management	16. Monitoring	17. User Account Management	18. Secure Infrastructure	19. Manage malware attacks	20. Protect infrastructure components	21. Physical security
EBA topics	**Governance**	X		X	X	X	X				X		X			X						
	Inadequate determination of Risk Appetite				X																	
	Inadequate/unapproved policies	X			X						X		X			X						
	Ineffective committee/organisational structures			X	X	X																
	Unclear mandates	X			X	X	X															
	ICT availability and continuity risks - Disruptive and destructive cyber attacks																		X	X		
	Disruptive and destructive cyber attacks																		X	X		
	ICT availability and continuity risks - ICT system failures										X	X							X			
	A loss of availability due to hardware failures											X							X			
	A loss of availability due to software failures and bugs										X	X							X			
	ICT availability and continuity risks - Inadequate capacity management								X	X				X								
	Inadequate capacity management								X	X				X								
	ICT availability and continuity risks - Inadequate ICT continuity and disaster recovery planning											X										
	Inadequate ICT continuity and disaster recovery planning											X										
	ICT change risks - Inadequate controls over ICT system changes and ICT development										X											
	Inadequate controls over ICT system changes and ICT development										X											
	ICT change risks - Inadequate ICT architecture		X	X																		
	Inadequate ICT architecture		X	X																		
	ICT change risks - Inadequate lifecycle and patch management						X							X								
	Inadequate lifecycle and patch management						X							X								
	ICT data integrity risks - Ill controlled data changes in the production ICT systems.										X											
	Ill controlled data changes in the production ICT systems										X											
	ICT data integrity risks - Ill designed and/or managed data architecture, data flows, data models or data dictionaries		X				X															
	Ill designed and/or managed data architecture, data flows, data models or data dictionaries		X				X															
	ICT outsourcing risks - Inadequate outsourcing governance														X		X					
	Inadequate outsourcing governance														X		X					
	ICT outsourcing risks - Inadequate resilience of third party or another Group entity services														X		X					
	Inadequate resilience of third party or another Group entity services														X		X					
	ICT outsourcing risks - Inadequate security of third party or another Group entity																X					
	Inadequate security of third party or another Group entity																X					
	ICT security risks - Cyber-attacks and other external ICT based attacks																X		X	X		
	Attacks on communication connections and conversations																X		X			
	Attacks performed from the internet or outside networks for different purposes																X		X	X		
	ICT security risks - Inadequate internal ICT security							X	X				X					X	X		X	
	Gaining unauthorised access to critical ICT systems from within the institution (Authentication)							X	X									X				
	The unauthorised storage or transfer of confidential information outside the institution												X						X		X	
	Unauthorised ICT manipulations due to inadequate ICT access management procedures and practices (Authorisation)							X										X			X	
	ICT security risks - Inadequate physical ICT security																				X	X
	Deliberate or accidental damage to physical ICT assets																					X
	Insufficient physical protection against natural disasters																					X
	Misuse or theft of ICT assets via physical access																				X	X
	Incident handling															X						
	Inadequate incident handling															X						
	Risk management		X	X	X												X					
	Inadequate identification of emerging risks			X	X																	
	Inadequate risk identification		X	X	X												X					
	Inadequate risk mitigation				X												X					

Disclaimer

Dit document van Van Lanschot Kempen Investment Management NV (VLK Investment Management) wordt u slechts ter informatie aangeboden en biedt onvoldoende informatie om een beleggingsbeslissing te kunnen nemen. De informatie in dit document is niet compleet zonder de mondelinge toelichting gegeven door een medewerker van VLK Investment Management.
VLK Investment Management heeft een vergunning als beheerder van diverse ICBE's en ABI's en is bevoegd om beleggingsdiensten te verlenen en staat als zodanig onder toezicht van de Autoriteit Financiële Markten. VLK Investment Management wil uitdrukkelijk voorkomen dat de benchmarks die gebruikt worden in dit document gepubliceerd of beschikbaar worden gemaakt voor het publiek in de zin van de Benchmarkverordening. Daarom is de informatie in dit document uitsluitend voor intern zakelijk en niet commercieel gebruik aan u ter beschikbaar gesteld. Gebruik van (de informatie uit) dit document anders dan voor de doeleinden als hierboven beschreven, is alleen geoorloofd na voorafgaande toestemming van VLK Investment Management

VAN LANSCHOT KEMPEN

INVESTMENT MANAGEMENT

Beethovenstraat 300
1077 WZ Amsterdam
P.O. Box 75666
1070 AR Amsterdam

T +31 20 348 80 00
vanlanschotkempen.com/investment-management