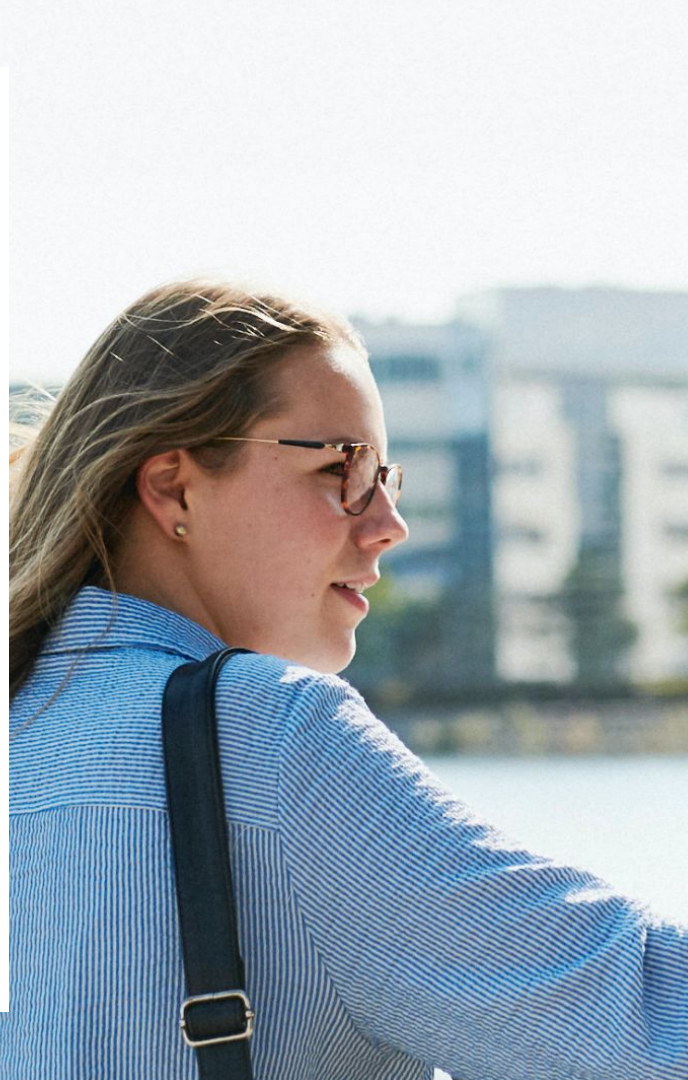


Visma Idella 'In Control'

Uw gids naar veilige, compliant
en controleerbare producten &
diensten van **Visma Idella**



Versie 7.3 - 2025



Inhoudsopgave

Beheerste bedrijfsvoering	3	DORA	21
Producten, diensten en doelgroepen	4	Privacy	23
Risicobeheersing	5	Niet-Financiële Risico's	25
Three lines model	6	Sira	26
Assurance	9	PUO Gericht toezicht DNB	27
DNB Good Practices	11	Duurzaamheid	28
Permanente educatie medewerkers	12	Business Operations team	29
Informatiebeveiliging	13	Meer informatie	30

De **beheerste bedrijfsvoering** van Visma Idella.

Dit document schetst de activiteiten van Visma Idella op gebieden die verband houden met de **zekerheid** en het **comfort** dat we bieden aan klanten die vertrouwen op onze SaaS-producten en BPO & PUO-diensten.

Onze gespecialiseerde focus op de financiële sector en financiële administraties, gecombineerd met een technologiegedreven aanpak, uitgebreide kennis en ruime ervaring binnen de Visma-groep, stellen ons in staat ervoor te zorgen dat we **de controle hebben over onze activiteiten**.

Als u vragen heeft over de inhoud van dit document, kunt u contact opnemen met uw Customer Success Manager of uw commerciële aanspreekpunt binnen Visma Idella.



Producten, diensten & doelgroepen

Technologie

VIPS
Pensions (a-a-S)

VIPS Retail
Investments (a-a-S)

VIPS
Disbursements

VIPS
Benefits

VIPS
Calculations

Pensioencommuni-
catie



Voor wie mogen we dit doen?

Gemeenten

Pensioen-
fondsen

Beleggings-
instellingen

Verzekeraars

Pensioen-
uitvoerders

Werkgevers
organisaties

APF

SPAWW

Universiteiten &
hogescholen

Operatie

PUO:
Digital Pension
Administration
as-a Service

Uitkeringen:
BPO
Disbursement
administration

APPA-BWW:
BPO
Benefits
administration

Risicobeheersing

Three lines model

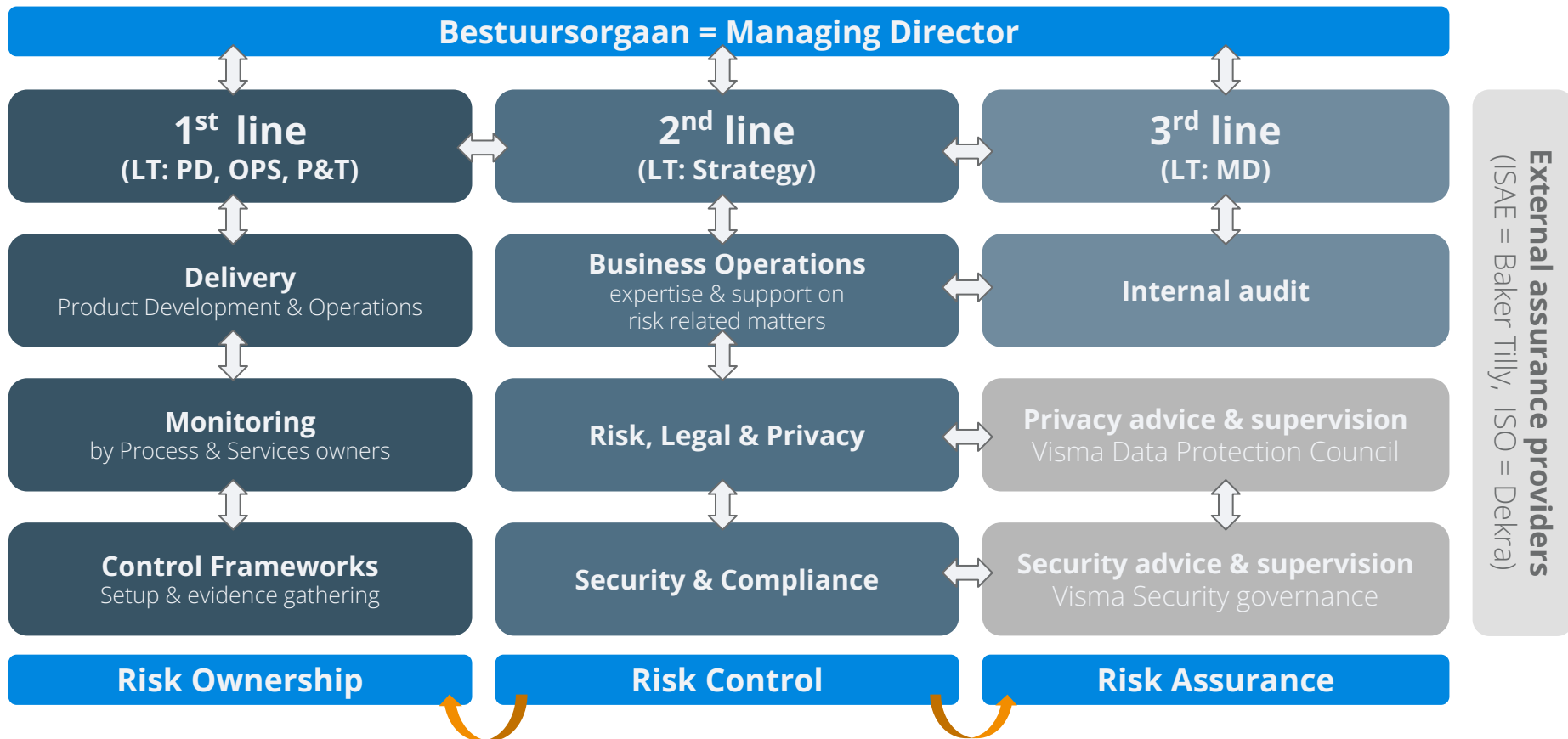
Voor het opzetten en uitvoeren van risicomanagementprocessen heeft Visma Idella het breed geaccepteerde 'three lines'-model toegepast op haar bedrijfsactiviteiten en organisatiestructuur.

Door de toepassing van dit model worden operationeel eigenaarschap, optimalisatie van de interne controles en de effectiviteit van controlemaatregelen gewaarborgd. Risicogebieden worden vanuit verschillende perspectieven benaderd.

Dit model waarborgt de onafhankelijke rol van auditactiviteiten en faciliteert belangrijke resultaten zoals ISAE-rapporten en TPM's voor DigiD-audits.

- **1e lijn:** De Delivery Unit is verantwoordelijk voor de tijdige, correcte en volledige uitvoering van operationele activiteiten, bijbehorende controlemaatregelen en bewijslevering.
- **2e lijn:** gescheiden van de dagelijkse bedrijfsvoering ondersteunt en adviseert het Business Operations-team over het optimaliseren van risicobeheersing, compliance, beveiliging en privacygerelateerde zaken.
- **3e lijn:** vanuit een onafhankelijke positie beoordelen en analyseren onze Internal Auditors periodiek de effectiviteit van controlemaatregelen zoals toegepast door de 1e en 2e lijn.

Risicobeheersing: Three lines model



Belanghebbenden **Pensioensector**

Of u nu een (bedrijfs-/organisatie)pensioenfonds, premiepensioeninstelling, pensioenuitvoerder of verzekeraar bent die pensioenoplossingen levert, **Visma Idella** doet er alles aan om u in staat te stellen te voldoen aan de eisen van wet- en regelgeving. Hierbij houdt zij rekening met door Good Practices, richtlijnen en documentatie opgesteld door:

- **De Nederlandsche Bank**
- **Pensioenfederatie**
- **Autoriteit Financiële Markten**



Audit activiteiten

Visma Idella kent verschillende soorten audits:

- **Interne audits** - onafhankelijke beoordelingen van de processen, de kwaliteit en de operationele effectiviteit van deze processen en van de controlemaatregelen die door de eerste en tweede lijn zijn opgezet.
Interne audits dragen bij aan het lerend vermogen door het verschaffen van inzicht aan management en het geven van input voor organisatieverbetering.
- **Externe audits** - Visma Idella houdt zich aan richtlijnen van wet- en regelgevers en communiceert transparant over de wijze waarop de kwaliteit van de dienstverlening wordt gewaarborgd.
Om die reden laat Visma Idella jaarlijks accountants en gecertificeerde auditors de relevant aspecten van producten en diensten beoordelen en certificeren.

Uw recht op controle en onderzoek

In gevallen waarin onze klanten gerechtigd zijn en reden hebben om hun recht op audit uit te voeren, is dit uitsluitend voorbehouden aan onafhankelijke en geaccrediteerde partijen. Aangezien Visma Idella aan veel organisaties diensten verleent, wordt elke audit zo opgezet dat er geen verstoring van de reguliere bedrijfsvoering voor andere klanten optreedt.

Alle audits dienen ruim van te voren te worden aangekondigd en zijn gebaseerd op een goed omschreven auditplan in overeenstemming tussen Visma Idella en de betrokken partij.
In lijn met de DNB Good Practices zijn het 'recht op onderzoek' en 'recht op audit' opgenomen in contracten met zowel klanten als onze leveranciers.

Assurance

Visma Idella verzorgt de assurance van uw uitbestede diensten door middel van ISAE 3000 en ISAE 3402 rapportages.

Door Visma Idella uitgebrachte ISAE-rapportages, zijn uitgevoerd conform de Richtlijn 3000 "Assurance-opdrachten"*) en Richtlijn 3402 "Assurance-rapportages"*) inzake beheersings- maatregelen bij een serviceorganisatie". Deze externe controlewerkzaamheden worden uitgevoerd door **Baker Tilly**.

*) Beide richtlijnen zijn vastgesteld door NOREA (Nederlandse Orde van Register EDP-auditors)

ISAE 3402 is specifiek gericht op het uitbesteden van processen en controlemaatregelen die relevant zijn voor de financiële verslaggeving en wordt voornamelijk toegepast voor BPO-gerelateerde diensten.

ISAE 3000 richt zich op processen die niet relevant zijn voor de financiële verslaglegging, zoals Service Level Management of Continuity Management en wordt voornamelijk toegepast voor IT/SaaS gerelateerde diensten.

Daar waar Visma Idella in het proces gebruik maakt van externe dienstverleners of subdienstorganisaties zijn met deze partijen contractuele afspraken gemaakt om periodiek TPM's (Third Party Memorandums) of ISAE-rapportages te ontvangen.

Beschikbare assurance & certificeringen

Technologie cluster



ISAE3000 VIPS
Software
Maintenance &
Support



DNB Security
Self Assessment
(Cobit58, incl.
uitbestedingen)



TPM DigiD
Audit &
Penetratie test



ISAE3402 BPO
Pensions
Administration



ISAE3402 BPO
Disbursement
Administration



Security:
ISO27001

Privacy:
Data Pro Code

De **gecombineerde assurance-rapporten** geven zekerheid over de gehele keten van uitbestede processen en activiteiten, vanuit zowel technologie als operationeel perspectief.

De sub-service organisaties Visma IT&C B.V. en Visma Raet maken via de **carve out methode** onderdeel uit van Visma Idella's assurance rapportages. **Baker Tilly** is de aangewezen externe accountant voor het afgeven van de ISAE verklaringen. De TPM verklaringen voor DigiD worden afgegeven door eveneens **Baker Tilly** en **2Control**.

Toepassing DNB Good Practices

DeNederlandscheBank



DNB Security Self Assessment (gebaseerd op Cobit58)



Right-to-Audit in onze contracten met klanten en leveranciers



Uitgebreide screening van alle werknemers vóór en tijdens indiensttreding



Periodieke en continue training van alle werknemers inzake AVG, integriteit en veiligheid



Gilde Wet- en Regelgeving als interne waakhond voor continue compliance producten en diensten



Informatieverstrekking over keten ten behoeve van aanmelding onderuitbesteding bij DNB

Permanente educatie medewerkers

Alle Visma Idella-medewerkers volgen minimaal jaarlijks diverse trainingen om hun kennis en vaardigheden inzake AVG, integriteit en veiligheid up-to-date te houden. Een overzicht van de trainingen:

- Cybersecurity awareness;
- Anti-corruptie/Code of Conduct;
- Privacybewustzijn.



Informatiebeveiliging



Informatiebeveiliging

Visma Idella heeft de verantwoordelijkheid en de wettelijke verplichting om veilige en beveiligde diensten te leveren. Wij zijn over de hele linie verantwoordelijk voor de beveiliging van klantgegevens.

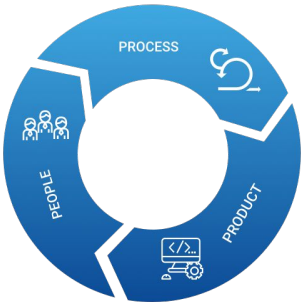
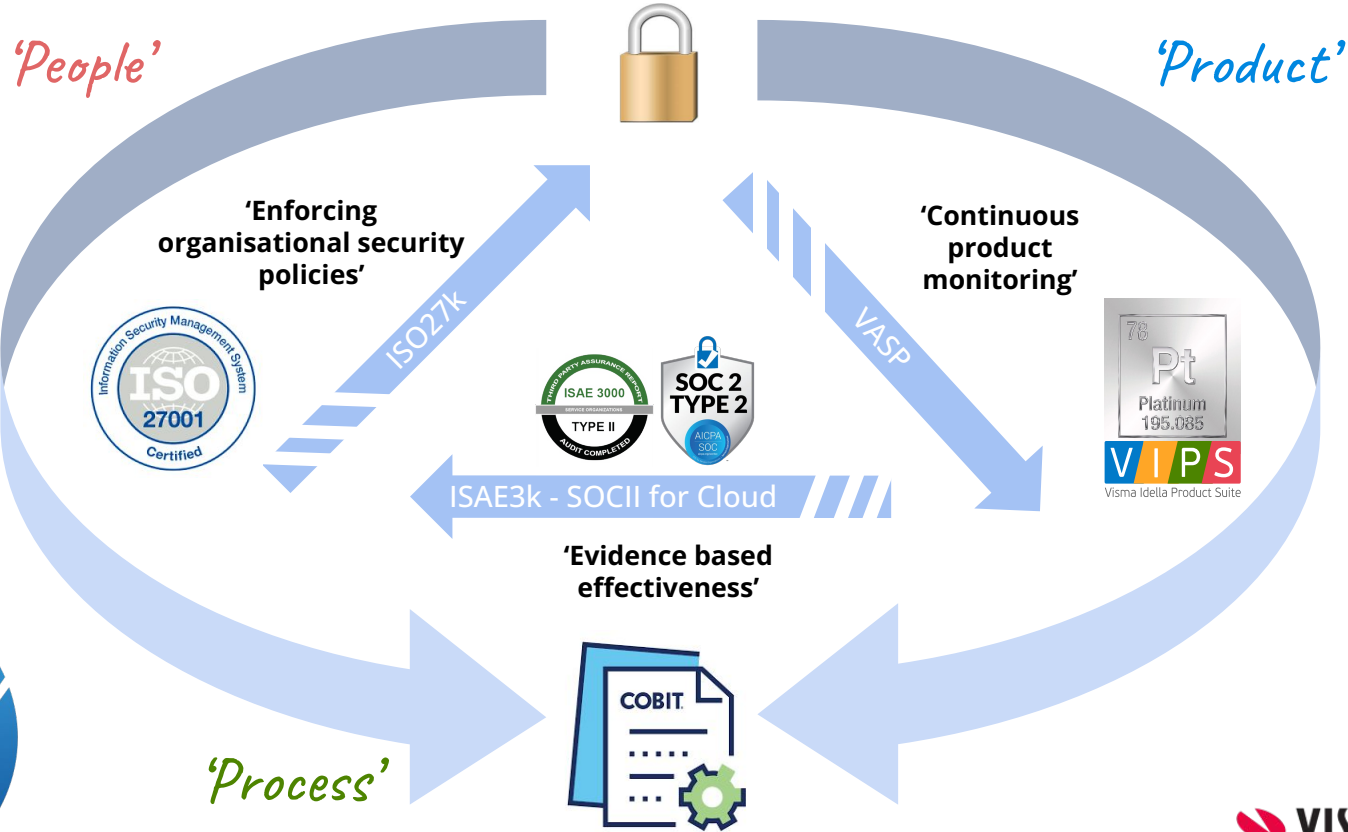
Beveiliging is geïntegreerd in alle onderdelen van onze complexe organisatie. Dit doen we om te waarborgen dat de gegevens van onze klanten, onze eigen gegevens en onze infrastructuur van topkwaliteit zijn. Dit is een basisvereiste voor al onze activiteiten en diensten. Het is nu en ook in de toekomst een van onze **primaire aandachtsgebieden**.

De aard van beveiligingsrisico's en cybercriminaliteit verandert voortdurend. In onze rol als leverancier van cloud oplossingen hebben wij **veiligheidsbewustzijn** in volledig in onze processen geïncorporeerd.



Visma security
awareness program

Visma Idella's **circulaire** security aanpak



Security standaard - ISO 27001

ISO/IEC 27001:2013 Annex A

Visma Idella heeft een **ISMS** (Information Security Management Systems) geïmplementeerd op basis van de toonaangevende internationale standaard **ISO/IEC 27001** en onderhoudt dit om:

- Gegevens te beschermen die van cruciaal belang zijn voor het bedrijf
- Risico's te beperken en een solide en constante uitvoering te garanderen
- Stakeholders en klanten vertrouwen te bieden

The ISO/IEC 27001 standaard beschrijft een proces voor **risicobeheer** waarbij mensen, processen en IT-systemen worden betrokken, en biedt daarmee een holistische benadering van **informatiebeveiliging**.

In 2023 heeft Visma Idella het **ISO 27001** certificaat behaald **voor de gehele dienstverlening**. Deze certificering bevestigt onze inzet voor best practices op het gebied van beveiliging en informatiebeveiligingsmaatregelen en -bescherming over de gehele linie van onze activiteiten.



Visma Application Security Program

Visma spant zich maximaal in als het gaat om de beveiliging van onze producten en diensten. Dit uit zich in het bedrijfsbrede programma VASP. VASP waarborgt veiligheid en privacy door middel van organisatorische, technische en fysieke maatregelen en omvat beleidslijnen, richtlijnen, procedures en technische systemen voor naleving van de beveiliging.

Deze maatregelen zijn ter bescherming van **vertrouwelijkheid, integriteit en beschikbaarheid van data alsmede de bestendigheid en wettelijke naleving** van onze producten en diensten.

Het beveiligingsniveau van een bepaald product of een bepaalde dienst is gebaseerd op een risicobeoordeling. Onze halfjaarlijkse **Security Self Assessment** (SSA) is de kern van beveiliging, privacy en gegevensbescherming in onze producten. De SSA wordt minstens jaarlijks uitgevoerd en omvat vereisten, aanbevelingen en beoordelingen ter beveiliging van toepassingen en naleving van de privacyregels.

Security in **assurancerapportages**

Visma Idella biedt zekerheid over informatie-beveiliging door middel van een verscheidenheid aan certificeringen en assurancerapporten. Ons raamwerk voor beveiligingscontrole is ontworpen om aan de Digital Operational Resilience Act (DORA) te voldoen en zo af te stemmen op de wettelijke vereisten die van toepassing zijn op ons klantenbestand.

DORA geeft het wettelijk kader waaraan voldaan moet worden om de integriteit, continue beschikbaarheid en veiligheid van de geautomatiseerde gegevensverwerking te garanderen.

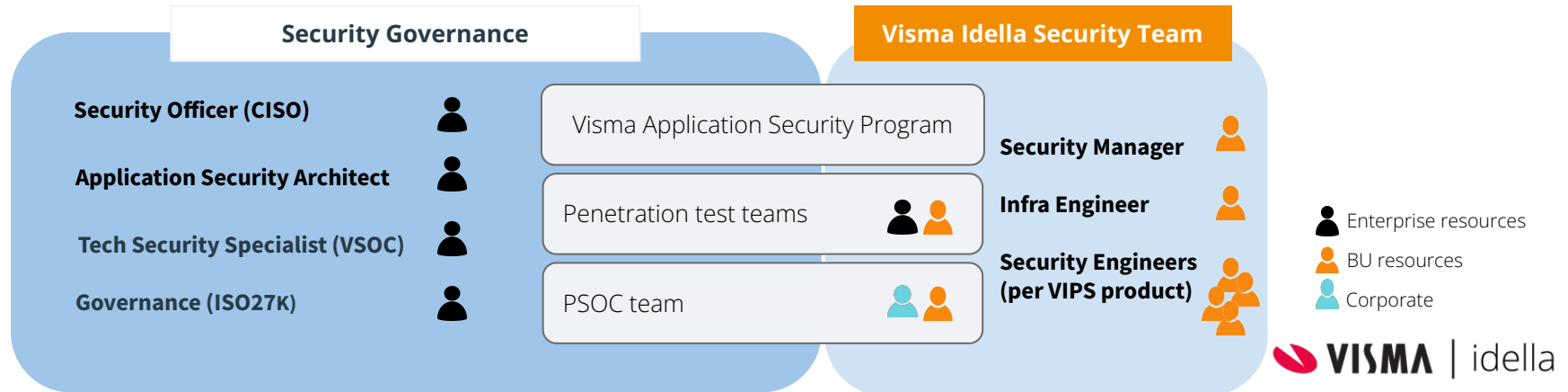
Het **DNB Security Self Assessment (SSA)** vormt in veel opzichten de kern van beveiliging, privacy en gegevensbescherming in onze producten.

Daarnaast faciliteert Visma Idella de DigiD-audits voor klanten die afhankelijk zijn van online producten. Organisaties die gebruik maken van DigiD moeten jaarlijks voldoen aan de verplichte DigiD-beveiligingsstandaard van Logius, opgesteld door NOREA. Organisaties met een DigiD-aansluiting worden jaarlijks getoetst op basis van het DigiD ICT-veiligheidsoordeel.

Security governance

Informatiebeveiliging zit in het DNA van elke Visma business unit. Voor elk VIPS-productontwikkelingsteam is dit een belangrijk onderdeel. Binnen elke divisie is een CISO (chief information security officer) aangesteld en in iedere board meeting met Visma wordt informatiebeveiliging behandeld als prioriteit voor onze product- en service-architectuur.

De **Security Manager** van Visma Idella is de eerstverantwoordelijke voor het plannen, leiden of coördineren van activiteiten om de informatiebeveiliging te waarborgen.



Aandacht voor maximale zekerheid: SOCII

Voor alle cloud-producten voor de pensioensector (o.a. pensioenadministratie en excasso) maken we in de periode 2023 - 2026, de overgang van SOCI ISAE3000-II naar SOCII assurance.

Hiermee garanderen we assurance van de hoogste categorie (in eerste instantie voor security & privacy).

Hierop aanvullend eisen we van alle onze cloud-producten, dat zij op Platinum niveau in onze security programma's acteren (VASP voor applicaties en VISP voor cloud-infra).

Onze huidige SOCI ISAE3000-II/ Cobit58 DNB SSA/ ISO27k & security programma's dekken reeds 70% van de SOCII eisen. De resterende 30% in kaart gebracht en ingevuld in People, Process & Product en op onze Product Roadmap ingekleurd.



Visma Idella's **DORA** DNA-string

Analyse beleid
rule books
ESA/ DNB

Classificatie &
rapportage
incidenten

Testen
weerbaarheid

Risicobeheersing
3e partijen



Gilde wet- en
regelgeving

DORA Task
force Visma

Impact
analyse

Implementatie &
exploitatie

Incidentafhandeling

De manier van werken van Visma Idella is

- Compliant met DORA
- Melding aan klant: binnen 24 uur (behoudens 'major incidents')

Het incidentafhandelingsproces bestaat uit 5 fasen:

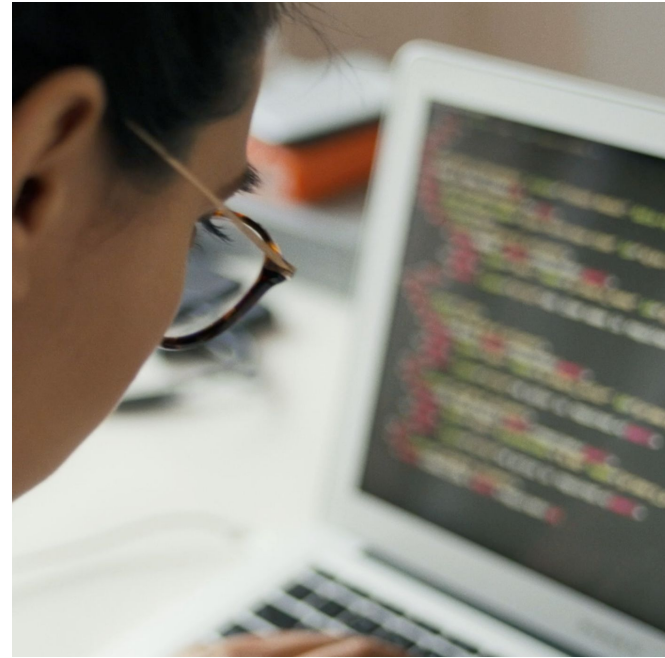
1. Melding ontvangen
2. Incident beoordeeld
3. Directe risicomitigatie
4. Incident opgelost
5. Rapportage, evaluatie en afsluiting van het incident



AUTORITEIT
PERSOONS-GEGEVENS

DeNederlandscheBank

Privacy



Privacy

Visma Idella levert diensten die voor veel van haar klanten een kritieke onderuitbesteding betreft. Het is in die rol als kritieke onderuitbesteder voor (onder toezicht staande) klanten essentieel, dat Visma Idella zich 24/7 inzet voor een veilige wijze van verwerking van data.

Toepasselijke wet- en regelgeving (niet limitatief):

- (Uitvoeringswet) Algemene Verordening Gegevensbescherming
- DORA
- NIS2
- Gedragscode Pensioenfederatie

Certificering(en)

Visma Idella is officieel gecertificeerd conform de Data Pro Code. De Data Pro Code is de eerste door de [Autoriteit Persoonsgegevens](#) erkende gedragscode als bedoeld in [artikel 40 AVG](#). (<https://scope-europe.eu/en/data-pro-code/public-register>).

Vertrouwelijkheid

- Is opgenomen in elke overeenkomst met klanten, leveranciers en (tijdelijke) medewerkers.
- Onze ontwikkelteams (en ook andere teams en medewerkers) krijgen aanvullende opleiding en ondersteuning, afgestemd op hun rol.

Rapportage **niet-financiële** risico's

Elk kwartaal informeren wij onze DPaaS/PUO-klienten, over de niet-financiële risico's met betrekking tot onze uitvoeringswerkzaamheden via onze NFR-rapportage.

De volgende **risicogebieden** komen hierin aan bod:

- strategie & omgeving
- uitbesteding
- informatietechnologie
- operationeel
- integriteit
- security
- legal & compliance



SIRA

Visma Idella streeft een **integere bedrijfsvoering** na. We handelen daarom in lijn met de [DNB Good Practice Integriteitsrisicoanalyse](#).

Jaarlijks voert Visma Idella een Systematische Integriteits- risicoanalyse (SIRA) uit. Op deze manier ondersteunen wij onze klanten in hun wettelijke verplichting om een integriteitsanalyse uit te voeren.

Tevens wordt op verzoek van Visma AS jaarlijks een 'Corruption Risk Assessment' uitgevoerd. Hierin wordt getoetst in hoeverre we handelen conform de [Anti-Corruption Policy](#) en de [Code of Conduct](#).

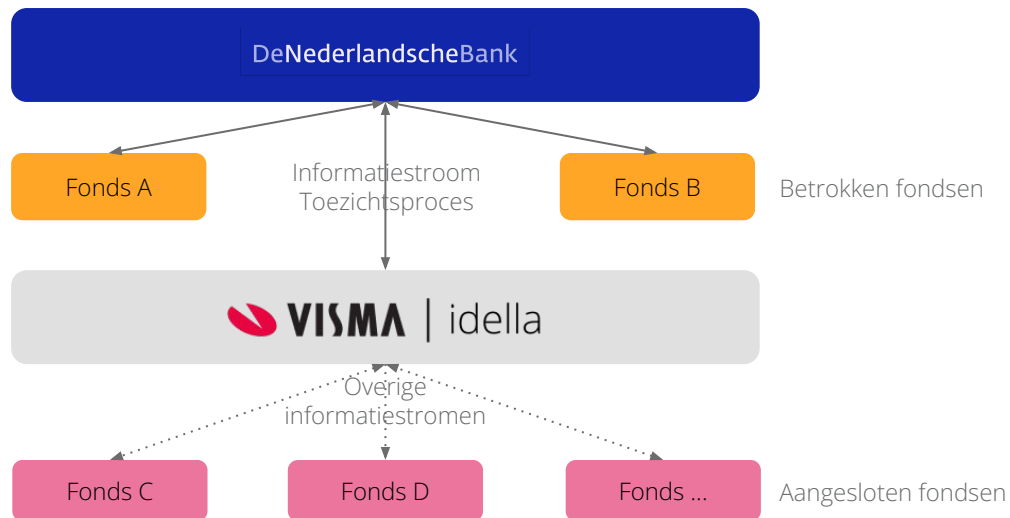


SIRA

PUO-gericht toezicht DNB

Als pensioenuitvoeringsorganisatie (PUO) raakt Visma Idella frequent betrokken in het toezicht door DNB op pensioenfondsen. Uiteraard verleent Visma Idella hieraan alle medewerking.

Gezien het feit dat onze dienstverlening (qua Operatie en Technologie) in hoge mate gestandaardiseerd is, delen wij de uitkomsten van dergelijke onderzoeken ook met Aangesloten fondsen.



Aandacht voor **duurzaamheid**: CSRD

In het kader van CSRD publiceren wij onze duurzaamheids- strategie inclusief meetbare doelen, duurzaamheidsbeleid en maatregelen in ons jaarverslag.

De implementatie van het **Visma Duurzaamheidsbeleid** is een eerste stap op weg naar een duurzame toekomst voor toekomstige generaties op een proactieve manier.

In 2021 startten we een doorlopend project om alle medewerkers bewust te maken van onze maatschappelijke verantwoordelijkheid. Vanaf 2023, compenseren wij actief de Scope 2 CO2 emissies.

Afvalstromen, reisgedrag, leveranciers, energieverbruik etc: alle data is beschikbaar. Wij verkleinen onze emissies ieder jaar.

Met CO2 neutraliteit onder handbereik compenseren we onze res-emissies met [Trees4All](#). Zo zijn wij de eerste SaaS leverancier en PUO in de pensioensector die **CO2 neutrale dienstverlening** levert!



Martijn de Vries
Strategy Director

Verantwoordelijk voor Visma Idella's
license-to-operate in 2e lijn, team management & strategische projecten
om continue doorontwikkeling en beheerste groei van onze organisatie
te waarborgen.

Corinna Angel
Sr. Legal Counsel &
DPO

2e lijns functie

Juridisch expert in
customer
contracting en
leveranciers-
contracten,
gecombineerd met
een sterke focus op
privacy.

Lilian Rolefes
Risk Manager

2e lijns functie

Verantwoordelijk voor
'PUO Gericht Toezicht',
risico & tactische
ketenregie DPaaS-
dienstverlening
richting leveranciers
en DNB.

Gerwin Dirkszager
Security Manager

2e lijns functie

Security & compliance
management en
beleidsvorming met
nadruk op
proceseigenaar-
schap ISO27k, VASP,
DNB SSA/ Cobit58 en
DigID.

Jan Riemer
Risk Manager

2e lijns functie

Ervaren
risicomanager, ziet toe
op de
risicobeheersing &
assurance die we
vanuit Visma Idella
leveren op
WTP-implementaties.

Sita Ramkhelawan
Sr. Internal Auditor

3e lijns functie

Senior Internal Auditor,
verantwoordelijk voor
assurance rapportages en
onafhankelijke audits. Direct
rapporterend aan Managing
Director/ bestuursorgaan.

Meer informatie

Hieronder treft u een aantal handige **links** voor meer achtergrondinformatie:

[Visma Trust centre](#)

[Code of conduct](#)

[Privacyverklaring](#)

[Duurzaamheid](#)

Op aanvraag verstrekken wij graag meer informatie over:

- Uitbestedingsbeleid
- Datakwaliteit
- Business continuity
- Informatiebeveiliging

Als u vragen heeft over de inhoud van dit document, kunt u contact opnemen met uw Customer Success Manager of uw commerciële aanspreekpunt binnen Visma Idella.

Ook kunt u uw vraag stellen via ons [contactformulier](#).



Entrepreneurial
Responsible
Dedicated
Inclusive

Make progress happen

 **VISMA** | idella