

GENOOTSCHAP VOOR RISICOMANAGEMENT | LEZING

AI Governance in de praktijk

Van *toezicht op AI* naar ***aantoonbaar in control*** — gezien vanuit de risicomanager

Hein van den Steenhoven

Managing Consultant — ARCAAS BV

Lezing voor het Genootschap Risicomanagement

Hein van den Steenhoven

Consultant Risk & Compliance | Auteur | Docent

Praktische Risk & Compliance-manager. 25+ jaar ervaring in de financiële sector, van werkvloer tot Senior Management. Hands-on, verbinder, vertaalt wettelijke eisen naar werkbare afspraken. Helpt bij het vastleggen van maatregelen die risico's verkleinen.

AUTEUR

Vier boeken op het vakgebied

- AI Governance in de praktijk
- Handboek Compliance
- Handboek Business Continuity Management
- Organisatie in verandering: de drie lijnen aan zet
- NOREA — reeks publicaties AI Governance 2026

PRAKTIJK

Recente opdrachten a.i.

- Pensioenfonds Horeca & Catering — Programmamanager DORA + Manager ORM
- Klaverblad Verzekeringen — Compliance Manager
- ANWB — 1e lijn Risk Manager + projectmanager Sanctiewet
- Yarden, Conservatrix, Nuvema — herstel onder DNB-toezicht

DOCENT EN SPREKER

Verbonden aan opleidingen

- Nyenrode (SPO)— Compliance
- Nederlands Compliance Instituut — Leergang compliance professional en AI Governance
- Governance Academy — AI Governance voor board en commissarissen
- Haagse Hogeschool — Masteropleiding Risicomanagement

EIGEN BEDRIJVEN

Co-founder sinds 2024

- ARCAAS — consultancy in audit, risk en compliance
- AuditNexus — IT-audit
- Mede-oprichter, directeur en aandeelhouder
- Eerder: directeur/partner van twee IT-bedrijven (data classificatie en media monitoring)

Voordat we beginnen — drie dingen over AI die de rest dragen

Drie punten die de rest van de bijeenkomst dragen

0 1

Hier

De vraag is niet meer 'of'.

AI zit al in je werk voor klanten — vaak verstopt in bestaande software. Niet óf, maar hoe beheerst.

0 2

Rekenmodel

Geen denker. Geen moraal.

AI voorspelt patronen — zonder bedoeling, besef of verantwoordelijkheid. En het kan overtuigend fout zijn.

0 3

Eromheen

Daar zit de governance.

AI is zo goed als de data, het ontwerp en de sturing eromheen. De techniek is zelden de governance-vraag — de keuzes erbij wél.

De hoofdboodschap van deze bijeenkomst

Vertrouwen in AI is geen *zachte kwestie*.
Het is de ***uitkomst in de dagelijkse praktijk*** van
aantoonbaar in control zijn.

*Dat is de stelling van vandaag. De feiten, het vertrouwen én de **wetenschap** wijzen dezelfde kant op — en daarna laat ik zien hoe je het met bewijs maakt.*

Vier delen, één conclusie

Feiten → vertrouwen → eisen → antwoord

INTERNATIONAL AI SAFETY REPORT 2026

01

Wat AI feitelijk doet — en waar het mis kan gaan

± 25 min

Mogelijkheden, drie soorten risico's, het bewijsdilemma

EDELMAN TRUST BAROMETER

02

Vertrouwen bepaalt de ruimte voor AI

± 15 min

Verskil in vertrouwen, vertrouwen opbouwen, draagvlak

DE TOEZICHTHOUDERS

03

Wat AFM, DNB, AP en ACM verwachten

± 15 min

Convergerende lat, grondrechten, governance vooraf

AI GOVERNANCE IN DE PRAKTIJK

04

Het antwoord — met bewijs onderbouwd

± 40 min

Dossier, samenhang, lastige keuzes, BIA, ketencontinuïteit, bewijs leveren

DEEL 01

Wat AI feitelijk doet

International AI Safety Report 2026 — 100+ experts, 30+ landen, onder voorzitterschap van Yoshua Bengio. De meest betrouwbare samenvatting van wat we nu weten over wat AI kan en welke risico's er zijn.

Wat veranderde sinds 2025 — en waar het misgaat

Sinds 2025: AI is sneller, breder en autonomer. De risico's vallen in drie soorten — elk een andere aanpak.

I

Misbruik door mensen

Een mens gebruikt AI verkeerd

- AI-inhoud: fraude, oplichting, beelden zonder toestemming
- Beïnvloeding & manipulatie (in tests net zo effectief als een mens)
- Cyberaanvallen — 77% van de zwakke plekken gevonden in één wedstrijd
- Bio/chemie — onduidelijk of de drempel voor beginners blijft

Governance-antwoord: Toegang controleren, misbruik opsporen, rapporteren

II

Storingen

Het systeem gaat zelf fout

- Betrouwbaarheid: dingen verzinnen, foute code, misleidend advies
- AI-agents vergroten het risico: ze handelen zelfstandig
- Verlies van controle: nog geen direct gevaar, wel een trend
- fairness en afwijken na verloop van tijd horen ook bij dit soort fouten

Governance-antwoord: Testen, in de gaten houden, terugvaloptie, mens-in-de-lus

III

Systeemrisico's

Brede effecten op de samenleving

- Werk: kennisbanen worden geautomatiseerd — onzeker hoe ver
- Zelfstandigheid: te veel op de tooling vertrouwen, minder zelf nadenken
- Apps met ingebouwde AI: tientallen miljoenen gebruikers
- Concentratierisico: afhankelijk van weinig aanbieders

Governance-antwoord: Denken in scenario's, kijken naar risico's in de keten en bij concentratie

Bron: International AI Safety Report 2026, §2 Risks. Let op: de EU AI-Act gebruikt 'systemic risk' in een striktere betekenis (alleen voor zeer grote frontier-modellen).

Het bewijsdilemma

Waarom governance méér moet zijn dan "we wachten op betere data"

TE VROEG REGULEREN

Maatregelen die niet werken vastleggen.

Regels op een verkeerd risicoprofiel, compliance-kosten zonder dat het beter werkt.

TE LAAT REGULEREN

Samenleving kwetsbaar voor echte schade.

Klanten worden benadeeld, oneerlijke uitkomsten, problemen in de keten — pas zichtbaar als ze al gebeurd zijn.

WAT DIT BETEKEN T

Governance op basis van bewijs, niet op basis van hype of angst.

Voor financiële instellingen: het antwoord op het dilemma is niet stilzitten of overreguleren. Het is **risico-proportioneel bewijs** organiseren: zwaar waar impact groot is, licht waar impact klein is.

De "evaluation gap": pre-deployment tests voorspellen de praktijk niet betrouwbaar. Modellen leren verschil herkennen tussen test en productie. **Dus: pre-market testen is niet genoeg — post-market monitoring wordt doorslaggevend.**

Vijf gevolgen voor organisaties

Van "experimenteren met AI" naar "kernproces met AI"

- | | | |
|----|--|--|
| 01 | Van assistent naar zelfstandige agent | Eerste generatie: GenAI-assistenten bij dossierwerk. Volgende: zelfstandige agents in KYC, claims, AML, krediet. Governance moet een grote stap maken. |
| 02 | Vooraf testen is niet genoeg | Het verschil bij beoordeling geldt ook voor jouw leverancier. Vertrouw niet alleen op de 'model card' — eis toezicht na livegang en het recht om audits te doen. |
| 03 | Keten wordt kritiek | Een handjevol frontier-labs heeft veel macht. Dezelfde fouten komen bij alle afnemers tegelijk terecht. In DORA / NIS2-taal: critical ICT third-party. Art. 25 bij elke model-update. |
| 04 | Fairness = betrouwbaarheid | De literatuur ziet 'ethische' fouten en 'technische' fouten niet meer apart. Verschillen tussen groepen zijn een vorm van modelfouten — stuur erop, niet eromheen. |
| 05 | De lastige keuze rond open-weight | Open-weight modellen (waarbij iedereen het model kan downloaden) zijn goedkoper en opener, maar de beveiligingen zijn eraf te halen. Voor sectoren met regels: er is duidelijk beleid nodig. |

Bron: Gartner, 'Top Data & Analytics Trends in Banking and Insurance for 2026' (feb 2026) — 79% van banken en 76% van verzekeraars verhoogt funding voor data & analytics; en 'Banking Predicts 2026'.

DEEL 02

Vertrouwen bepaalt de ruimte

Edelman Trust Barometer — jaarlijks onderzoek onder 30.000+ deelnemers in 28 landen. De standaard voor vertrouwen in instellingen.

Acceptatie is geen techniek- maar een legitimiteitsvraag

Het verschil in vertrouwen loopt langs inkomens — en dat bepaalt of mensen AI accepteren

VERTROUWEN IN INSTELLINGEN

63 vs 48

Hoge inkomens (63) tegenover lage inkomens (48)

Een vast verschil van 15 punten in vertrouwen in bedrijven, overheid, NGO's en media.

WIE DENKT DAT AI HEM/HAAR ACHTERLAAT

54% vs 31%

Lage inkomens (54%) tegenover hoge inkomens (31%)

Generatieve AI voelt voor de ene helft als kans, voor de andere als bedreiging. Dit voorspelt weerstand om AI te gebruiken.

EFFECT VAN GOED VERTROUWEN OPBOUWEN

+18

49 → 67 bij lage inkomens

Als instellingen actief uitleg, fairness en verantwoording bieden, stijgt het vertrouwen flink — vooral bij wie het hard nodig heeft.

Bron: Edelman Trust Barometer — groepen 'hoge inkomens' tegenover 'lage inkomens' in G-7 + NL. Cijfers afgerond.

Van feiten en vertrouwen naar het antwoord

AI SAFETY REPORT

Feiten

AI wordt sneller, komt dichterbij kernprocessen, en testen vooraf is niet genoeg.



EDELMAN

Vertrouwen

Vertrouwen in de instelling bepaalt of mensen AI accepteren. Draagvlak ontstaat niet vanzelf.



GOVERNANCE

Antwoord

Aantoonbaar in control. Drie ankers, twee bewijslijnen, vier stappen. Gemeten, niet beloofd.

Twee bronnen stellen dezelfde vraag scherp — eerst de toezichthouders, dan het antwoord.

DEEL 03

Wat verwachten de toezichthouders

AFM, DNB, AP en ACM — één convergerende lat: governance vooraf, niet achteraf.

Wat DNB en AFM echt verwachten — vier uitgangspunten voor toezicht

Uit 'De impact van AI op de financiële sector en het toezicht' (DNB & AFM): het toezicht is technologie-neutraal — bestaande normen blijven daarom volledig gelden bij gebruik van AI

VIER UITGANGSPUNTEN VOOR TOEZICHT

01

Technologie-neutraal toezicht: doelen en normen staan los van de techniek en gelden volledig bij AI — **integere en beheerste bedrijfsvoering**, zorgplicht, productontwikkeling, normen tegen te veel krediet.

02

Passend bij het risico: hoe zwaar het toezicht is, hangt af van het belang van het proces en de risico's — zwaar waar de gevolgen groot zijn, licht waar ze klein zijn. Hoog-risico AI (krediet, premiebepaling levens/zorg) krijgt extra eisen; andere AI wordt aangemoedigd om vrijwillig te voldoen.

03

Gericht op de keten: het toezicht kijkt naar invoer (data-governance, vooroordelen), verwerking (model, uitlegbaarheid, stevigheid) en uitkomst (klantbelang, openheid, gelijke behandeling) — plus governance over alles heen en sterk staan in de praktijk.

04

Gericht op grondrechten: voor hoog-risico AI wordt een effectbeoordeling op grondrechten verplicht (FRIA). Gelijke behandeling en bescherming van gegevens vragen bijzondere aandacht — ook voor verschil dat indirect ontstaat via tussenliggende kenmerken.

DRIE DOORLOPENDE DISCUSSIES — OOK BINNEN HET TOEZICHT

Het normenkader moet waar nodig duidelijker worden

DNB & AFM geven aan: bestaande normen zijn van toepassing, maar de uitleg bij AI vraagt om verdere richtlijnen — het liefst gelijk op EU-niveau, voor gelijk toezicht en een gelijk speelveld.

Balans tussen verantwoord gebruik en ruimte voor innovatie

Scenario-analyse in het rapport: een goed evenwicht tussen meegroeierende regels en innovatie geeft de beste uitkomst. Onevenwicht leidt tot 'AI winter' (te veel regels) of 'AI zonder remmen' (te weinig regels).

Afhankelijkheid van vooral niet-Europese AI-leveranciers

Het rapport noemt dit duidelijk als geopolitiek thema. Een kleine groep technologiepartijen + inkoop van dezelfde modellen → systeemrisico's komen bij veel instellingen tegelijk naar boven. Concentratierisico wordt onderwerp van toezicht.

Bron: DNB & AFM, 'De impact van AI op de financiële sector en het toezicht' — hoofdboodschappen + hoofdstuk 2 (toezicht en wetgeving). Het sectorale AI-Act-toezicht ligt voor de financiële sector in principe bij AFM en DNB; daarnaast houdt de AP cross-sectoraal toezicht op de AVG en coördineert zij het AI- en algoritmetoezicht (DCA).

De AP-lens — AI is ook een grondrechten- en machtsvraagstuk

AFM en DNB vragen: ben je aantoonbaar in control?
De AP vraagt: kan de mens het ***begrijpen en aanvechten***?

Non-discriminatie

AI kan groepen anders behandelen, ook indirect via proxies.
De AP toetst of uitkomsten eerlijk en controleerbaar zijn.

Autonomie & verweer

De mens mag niet volledig aan het systeem onderworpen zijn: recht op uitleg, menselijke tussenkomst en bezwaar.

Transparantie van macht

Wie AI inzet kan mensen classificeren, sturen en voorspellen. Toezicht gaat ook over grip, uitleg en bescherming.

Eén AI-systeem, meerdere toezichthouders

Een instelling krijgt niet één toezichtbril maar meerdere tegelijk.

0 1

AFM & DNB

Financieel toezicht

Soliditeit, marktintegriteit, zorgplicht en beheerste bedrijfsvoering — technologie-neutraal, ook bij AI.

V R A A G

Ben je in control?

Sectoraal markttoezicht op hoog-risico AI

0 2

AP / DCA

Grondrechten & data

AVG, uitlegbaarheid, non-discriminatie, persoonsgegevens en autonomie — cross-sectoraal.

V R A A G

Kan de mens het aanvechten?

Coördineert het AI- en algoritmetoezicht (DCA)

0 3

ACM

Consument & markt

Consumentenbescherming, misleiding en platform- en markteffecten — o.a. chatbots, samen met de AP.

V R A A G

Wordt de consument misleid?

Gezamenlijke toezichtactie met AP en RDI

0 4

RDI

Digitale infrastructuur

Producttoezicht en technische veiligheid van digitale producten en infrastructuur onder de AI-Act.

V R A A G

Is het product veilig?

Markttoezicht op AI-producten in de keten

Waarom dit één governance is, geen vier: dezelfde toepassing wordt door meerdere toezichthouders bekeken vanuit verschillende lenzen. Één dossier dat al die lenzen bedient, voorkomt vier keer werk en tegenstrijdige antwoorden — de toezichthouders stemmen onderling af. Eén dossier dat al die lenzen bedient, is je dekkingsbewijs.

AFM, DNB, EIOPA én AP — 'governance vooraf, niet achteraf'

Vier toezichthouders, één boodschap: wachten tot business en IT hebben uitgerold is te laat. De vier punten hieronder zijn geen losse zorgen — het zijn signalen van dezelfde reactieve houding

- | | | |
|-----------|--|---|
| 01 | Signaal 1: bestuur en RvC krijgen het 'ter kennis' | AI-dossiers komen pas bij de top als ze al klaar of live zijn. De vraag wordt goedkeuren, niet sturen. Zonder vroege betrokkenheid mist het bestuur de AI-kennis — én de positie — om bij te sturen. |
| 02 | Signaal 2: tweede en derde lijn rapporteren over werk dat al klaar is | Risk, compliance en audit worden ingeschakeld na de 1e lijn — dan zijn de keuzes al gemaakt. Zonder eigen AI-kennis én zonder vroege positie wordt rapportage óf te algemeen om te sturen, óf te technisch om bij het bestuur te landen. |
| 03 | Signaal 3: beheersing moet achter de feiten aan rennen | Business start, IT en 2e lijn volgen. Zonder vooraf vastgestelde toelatingseisen, rollen en bewijsmiddelen wint snelheid élk gesprek — en worden incidenten pas zichtbaar als ze al gebeurd zijn. |
| 04 | Signaal 4: DORA / NIS2 en BCM pas in beeld na het incident | Risico's bij AI-leveranciers en ketencontinuïteit worden los van AI-governance beheerd — tot er uitval is. Proactief: critical ICT third-party én BCM (RTO/RPO, terugvaloptie) vastgelegd vóór livegang. |
| 05 | De gezamenlijke conclusie | Alle vier de signalen komen neer op hetzelfde: governance is reactief ingericht terwijl AI proactief beweegt. Toezichthouders verwachten niet 'meer beleid' — ze verwachten dat governance vóór livegang klaar staat, niet erná wordt ingeregeld. |

DEEL 04

AI Governance in de praktijk

De basis. De samenhang. De vertaling. De lastige keuzes.

AI-solutionisme — wat de wetenschap nu bevestigt

AI faalt zelden op de *techniek*.

Het faalt op het ***oordeel, de sturing en de governance*** eromheen.

*Precies de stelling van het begin, nu onderbouwd. Henry Adobor (Organizational Dynamics, 2026) noemt dit AI-solutionisme: AI kiezen vóór het **probleem** scherp is. Vijf principes vertalen het meteen naar de praktijk.*

Drie ankers — voor élk AI-systeem

Het werkmodel onder élke AI-toepassing — drie vaste vragen: welke rol, welke risicoklasse, welk bewijs?

0 1

Rol

Wie zijn wij in de keten?

Aanbieder, deployer, importeur of distributeur — soms meerdere tegelijk. Bepaalt welke plichten gelden onder de AI-Act.

0 2

Risicoklasse

Hoe zwaar weegt dit systeem?

Verboden, hoog, beperkt of minimaal. In de financiële sector: krediet, levens- en zorgpremiebepaling vaak hoog-risico.

0 3

Bewijs

Wat ligt er met bewijs op tafel?

AI-register + review-evidence-set. Zonder allebei: het systeem bestaat voor governance niet.

De vijf principes van Adobor — gegroepeerd onder de drie ankers

Adobor (2026) gekoppeld aan het werkmodel — elk principe valt onder één anker: rol, risicoklasse óf bewijs

ROL

Welke rol en verantwoordelijkheid onder de AI-Act.

01 Begin bij het probleem

Niet uit te leggen zonder de tool te noemen? Eerst je doel en rol — dan pas de techniek.

02 Pilots zijn om te leren

Stoppen of herontwerpen is een legitieme, bestuurlijke uitkomst — geen nederlaag.

RISICOKLASSE

Hoe zwaar het systeem weegt — verboden tot minimaal.

03 Stem toezicht af op het risico

Zwaardere gevolgen voor mensen of rechten → steviger toezicht.

05 Opschalen is een besluit

Nieuwe schaal of context verandert de klasse → opnieuw beoordelen (art. 25).

BEWIJS

Aantoonbaar in de review-evidence-set.

04 Bescherm menselijk oordeel

Mens-in-de-lus met echte ruimte en escalatie; het override-log is je bewijs (art. 14).

Productieve frictie — governance die 'stop' durft te zeggen

Niet minder enthousiasme, maar bewuste remmen tegen schijnzekerheid

0 1

Probleemgate

Lossen we een echt probleem op?

Geen AI zonder scherp probleem én een serieus no-AI-alternatief. Kun je het probleem niet zonder de tool uitleggen? Nog niet starten.

0 2

Exit- & stopcriteria

Mag het ook misgaan?

Pauzeren, aanpassen of stoppen is vooraf gelegitimeerd — een leeruitkomst, geen nederlaag. Vastgelegd in het pilotcontract.

0 3

Portfolio & besluitlog

Zien we het geheel?

Pilots, schaduw-AI en dubbele initiatieven samen bewaken. Leg vast waarom door / aan / stop — en stuur bij op foute aannames (CAPA).

Het verband: de probleemgate is de ingang van het dossier; besluitlog en CAPA voeden register en reviewset.

Rol onder de AI-Act — andere rol, andere zwaarte

De zaal kent de rollen. Waar het in de praktijk knelt: meerdere rollen tegelijk en art. 25.

ROL	BESCHRIJVING	KERNPLICHTEN AI-ACT	FOCUS
Aanbieder	<i>Bouwt AI of past AI flink aan</i>	Technische documentatie, conformiteitsbeoordeling, QMS, monitoring na livegang, EU-registratie hoog-risico.	Documentatie, testen, conformiteit
Deployer	<i>Gebruikt AI in eigen processen</i>	Gebruik volgens instructies van de aanbieder, echte menselijke controle, FRIA bij hoog-risico, incidenten melden.	Uitleg, HITL, monitoring
Importeur / Distributeur	<i>Brengt AI naar of door de EU</i>	Conformiteit controleren, CE-markering, meldplicht. Bij wezenlijke wijziging → je wordt aanbieder (art. 25).	Keten, auditrechten, art. 25

Waar het in de praktijk wringt: een AI-leverancier doet een model-update (nieuwe trainingsdata, nieuwe context) — formeel blijft jouw organisatie deployer, maar feitelijk is er een wezenlijke wijziging. Wie bewaakt de art. 25-gate wanneer jij geen zicht hebt op wat de leverancier doet?

Zonder dossier geen governance

Vastleggen is geen administratie — het is de basis waar al het andere op rust

Wat je niet kunt terugvinden,
kun je niet besturen.

En wat je niet kunt aantonen,
kun je niet auditen.

DE REDENERING IN DRIE STAPPEN

01

Beleid, visie en uitgangspunten zijn niet genoeg

Veel organisaties hebben beleid. Wat ontbreekt is het spoor van bewijs: welk systeem draait, wie is eigenaar, welke controles horen erbij.

02

Zonder dossier geen zinvol gesprek

Over fairness, evenredigheid of menselijk toezicht kun je pas echt praten als vastligt welke data, welke versie en welke controles er zijn.

03

Zonder dossier geen toezicht na livegang

Monitoring, incidenten en CAPA's zijn niet te volgen als niet duidelijk is welke versie draaide, welke data is gebruikt en welke controles hadden moeten werken.

*Daarom is de eerste vraag niet 'hebben we beleid?' maar **'hebben we een dossier dat klaar is voor audit?'***

Het governance-dossier: drie hulpmiddelen

Crosswalk geeft het kader, register vult per systeem in, reviewset bewijst dat het werkt

0 1

Crosswalk

Wie doet wat — voor alle systemen

Het kader voor de hele organisatie. Per wettelijke eis: welk proces, welk bewijs, welke eigenaar. Geldt voor élk AI-systeem.

0 2

Register

Wat hebben we — per systeem

Per AI-toepassing: doel, rol, risicoklasse, eigenaar, links naar bewijs. Het overzicht waarmee bestuur en toezicht weten wat er draait.

0 3

Reviewset

Werkt het ook — in de praktijk

Cijfers, logs, voorbeelden, overrides, CAPA's. Het bewijs dat het systeem in de praktijk doet wat het op papier zou moeten doen.

Het verband: *crosswalk = wat moet, register = wat we hebben, reviewset = bewijs. Ditzelfde dossier zit achter agentie AI, productieve frictie en de regimes.*

De crosswalk — van wet naar proces naar bewijs naar eigenaar

Wie doet wat? De wegwijzer voor compliance: geen dikke map, maar een spoor dat je kunt volgen

EIS — WAT	PROCES — HOE → per systeem in het REGISTER	BEWIJS — WAARMEE → getoetst in de REVIEWSET	EIGENAAR — WIE
Datagovernance	Datasheet invullen; grondslag, opt-out en doorgifte bij training	Datasheet, datakwaliteit + trainings-/doorgifteafspraken	Data Steward, Privacy Officer
Model governance	Model card + bias-/fairnesstoetsing bijhouden	Model card + fairnessmethodiek (groepen, drempels)	Data Science, Model Owner
Logging & traceerbaarheid	Invoer, uitkomst, modelversie en fouten loggen	Logboek, uittreksel uit log, bewaarbeleid	IT Operations, Security
Openheid, uitleg & verweer	AI-meldingen, recht op uitleg (algemeen + persoonlijk) en bezwaar	Kanaal-matrix + recht-op-uitleg-dossier, bezwaarroute	Communicatie, IT
Menselijk toezicht (art. 14)	Besliskaart, override-KPI + AI-geletterdheid (rolgericht)	Overridelog, KPI-rapport + AI-literacy-matrix	Proceseigenaar, 2e lijn
Incident- & CAPA-proces	Vastleggen, onderzoeken, sluiten met aantoonbaar effect	Incidentlog, CAPA-overzicht met effect	Risk, 2e lijn, auditcommissie

Zonder crosswalk: vertaalt elk team regels op zijn eigen manier — ruis, dubbel werk, onduidelijkheid. **Met crosswalk:** van eis naar proces naar bewijs naar eigenaar doorklikken.

Het AI-register — het overzicht per systeem

Het process / hoe (opzet en bestaan)? Geen lijstje, maar een hulpmiddel voor sturing: wat draait, wie is eigenaar, welk bewijs hoort erbij?

VELDEN VAN EEN COMPLEET AI-REGISTER

Systeemnaam / ID	Unieke kenmerk van de AI-toepassing
Doel & beschrijving	Wat doet het systeem en waarom wordt het gebruikt?
Rol organisatie	Aanbieder, deployer, importeur of distributeur
Risicoklasse	Verboden / hoog / beperkt / minimaal — met onderbouwing
Menselijk toezicht	Hoe is menselijk toezicht in de praktijk geregeld?
Databronnen	Welke data wordt gebruikt en waar komt die vandaan
Transparantie & labeling	Waar en hoe worden gebruikers geïnformeerd
Logging & retentie	Wat wordt gelogd, hoe lang bewaard, wie heeft toegang
Laatste review & open CAPA's	Wanneer laatst getoetst, welke acties lopen
Links naar bewijsstukken	AIA/FRIA/DPIA, datasheet, model card, kanaal-matrix
Recht op uitleg & verweer	Algemene + persoonlijke uitleg, bezwaarroute en doorlooptijd
AI-geletterdheid & chatbots	Rolgericht opleidingsniveau; bij chatbot: herkenbaar + escalatie naar mens

VOORBEELD | VERZEKERAAR — SCHADE-TRIAGE

Voorbeeld van één ingevulde regel uit het register

Systeem	Schade-triage AI
Doel	Schademeldingen ordenen op spoed en moeilijkheid
Rol organisatie	Deployer
Risicoklasse	Hoog risico
Datasheet	Versie 1.4
Model card	Versie 2.1
Logging	Invoer, uitkomst, modelversie, afwijken door medewerker
Transparantie	AI-melding in klantportaal, uitleg op B1-niveau
Laatste review	12 mei 2026
Open CAPA's	2
Eigenaar	Product Owner Schadebehandeling

De review-evidence-set — bewijs dat het werkt

Het bewijs, de werking. Het register zegt wat er zou moeten zijn. De reviewset laat zien of het ook echt zo werkt.

ONDERDELEN VAN DE REVIEW-EVIDENCE-SET

fairness & drift	Per doelgroep, met drempels, trend en CAPA als de drempel wordt overschreden
Prestaties	Nauwkeurigheid, precision/recall per situatie; trend sinds livegang
Override-KPI	Hoe vaak wijkt de mens af van AI — is dat te hoog of te laag?
Overridelog (voorbeelden)	Concrete voorbeelden: wat was het advies, waarom afwijken, wat de uitkomst was
Klachten & incidenten	Aantal, soort, koppeling aan CAPA, effect van de actie
Uitleg & labels	Wat ziet de gebruiker echt? In elk relevant kanaal — screenshots, voorbeelden
Logvoorbeelden	Voorbeeld dat je terug kunt halen: invoer → uitkomst → afwijken → resultaat
Mens-in-de-lus	Besliskaart, bevoegdheid, tijd — bewijs dat niet alleen op papier bestaat
Verbeteracties die nog open staan	Wat staat nog open, termijn, eigenaar, status
Recht-op-uitleg-dossier	Algemene + persoonlijke uitleg bij een echt besluit; doorlooptijd verzoeken
AI-geletterdheid & chatbot-escalatie	Literacy-matrix met toetsing per rol; escalatielogs van chatbot naar mens

HET VERSCHIL

Register: wat er zou moeten zijn.

Reviewset: bewijs dat het ook werkt.

Voor de IT-auditor: met het register toets je **opzet en bestaan**. Met de review-evidence-set toets je **werking**.

DE HARDE REGEL

Ontbreekt register of reviewset? Dan is het systeem niet klaar voor audit — hoe goed het beleid of de bedoeling ook is.

Wat zit er in het dossier? Vier kerndocumenten

Datasheet, model card, logging-plan en kanaal-matrix — de inhoud van register en reviewset

I Datasheet

De grondstofkaart

Welke data, herkomst, kwaliteit, representativiteit, privacy, bewaren. Bij training ook: grondslag, opt-out en doorgifte buiten EU.

Auditvraag: Kent de organisatie haar data echt? Is er een ritme voor herbeoordeling?

II Model card

De machinekaart

Naam/versie, algoritme, trainings-/validatiedata, prestaties, fairnessmethodiek (groepen, drempels), uitleg, versiebeheer.

Auditvraag: Is de modelversie herleidbaar? Ligt de relatie tussen trainingsdata en productieversie vast?

III Logging & retentie

Het geheugen

Invoer, uitkomst, modelversie, afwijken door medewerker, fouten, toegang. Hoe lang bewaard, wie heeft toegang, wanneer verwijderd.

Auditvraag: Kunnen we een specifiek AI-besluit reconstrueren? Is het retentiebeleid nageleefd?

IV Kanaal-matrix

De kaart over openheid

Per kanaal (web, app, brief, chat, dashboard): AI-melding, recht op uitleg en bezwaarroute; bij chatbot herkenbaar + escalatie naar mens.

Auditvraag: Is de AI-melding in alle kanalen consistent, in B1 en zichtbaar vóór interactie?

Het governance-dossier in één oogopslag

Drie hulpmiddelen, vier kerndocumenten — zo hangt het samen

CROSSWALK het kader voor de hele organisatie
per wettelijke eis → welk proces → welk bewijs → welke eigenaar

01 — REGISTER

Wat hebben we?

Per AI-systeem: doel, rol, risicoklasse, eigenaar, recht-op-uitleg, AI-geletterdheid, bewijs.

02 — REVIEWSET

Werkt het ook?

Cijfers, logs, overrides, klachten, recht-op-uitleg-dossier, literacy, CAPA's.

VIER KERNDOCUMENTEN — DE INHOUD VAN REGISTER EN REVIEWSET

DATA

Datasheet

Welke data, herkomst, kwaliteit, bewaren; trainingsgrondslag & doorgifte.

MODEL

Model card

Naam/versie, type algoritme, prestaties, fairnessmethodiek.

GEHEUGEN

Logging-plan

Wat wordt gelogd, hoe lang bewaard, wie heeft toegang.

OPENHEID

Kanaal-matrix

Per kanaal: AI-melding, recht op uitleg, bezwaar; chatbot-escalatie.

Mist één van de vier documenten of één van de drie hulpmiddelen? Dan is het dossier niet klaar voor audit.

Vier regimes, één AI-systeem

De toezichthouder kijkt naar de samenhang. Je klant beheert ze nog vaak apart.

0 1

AI-Act

Plichten die alleen voor AI gelden

Rol (aanbieder/deployer), risicoklasse, menselijk toezicht, openheid, FRIA, registratie.

WERKING

Hoog-risico: 2 aug 2026

Alle AI-toepassingen — verdeeld naar risico

0 2

DORA / NIS2

Sterk staan in de dagelijkse praktijk

Beheer van ICT-risico, incidenten melden, testen, critical ICT third-party — óók AI-leveranciers.

WERKING

Van kracht: 17 jan 2025

Elke AI-leverancier valt onder het ICT-TP-regime

0 3

AVG

Rechten rond persoonsgegevens

Rechtmatigheid, doelbinding, DPIA, rechten van betrokkenen, art. 22 (besluit zonder mens).

WERKING

Onverminderd van kracht

Speelt zodra er persoonsgegevens in het AI-proces zitten — toezicht: AP

0 4

Uitbesteding

Regels per sector

EBA/EIOPA/DNB richtlijnen voor uitbesteding, materiële uitbesteding, exit-strategie, concentratierisico.

WERKING

Bestaande verplichting

Speelt bij AI bijna altijd — materieel zodra de functie kritiek is

Waarom dit één gesprek is, geen vier: één AI-systeem in krediet of claims raakt tegelijk de AI-Act (hoog-risico), DORA (ICT third-party en incident reporting), AVG (art. 22 ADM en DPIA) en outsourcingbeleid (materiële uitbesteding). Wie dit in vier losse werkstromen beheert, betaalt vier keer en krijgt drie keer de verkeerde uitkomst.

AI valt bijna altijd onder het uitbestedings- en DORA / NIS 2-regime

Niet élk AI-gebruik is materiële uitbesteding — maar zodra het een kritieke of belangrijke functie raakt, geldt het regime volledig

WAT DORA / NIS2 VAN JE VERWACHT BIJ EEN AI-LEVERANCIER

Register van ICT third-parties	AI-leveranciers horen in je ICT-TP-register — ook kleine SaaS-AI-tools
Beoordeling van materialiteit	Is deze AI-leverancier kritiek? Dan zwaarder regime, meldplicht aan toezichthouder
Wat in het contract moet staan	Auditrechten, SLA's, exit-strategie, toegang tot data, onderuitbesteding, termijnen voor incident melden
Doorlopend in de gaten houden	Prestaties, beschikbaarheid, incidenten, wijzigingen bij de leverancier
Stoppen en overdraagbaarheid	Kun je weg als het moet? Welke data krijg je mee? Hoe lang duurt de overgang?
Concentratierisico	Wat als dezelfde frontier-provider door jou én je sectorgenoten wordt gebruikt?

WAAR AI HET BIJZONDER INGEWIKKELD MAAKT

Model-updates als 'stille wezenlijke wijziging'

Leverancier past trainingsdata, fijnafstelling of beveiligingen aan zonder dat je het merkt. Art. 25 AI-Act geldt dan, maar jij ziet het niet.

Audit is bij frontier-providers zelden volledig

Hoe ga je om met een provider die zegt: 'dit model is van ons, geen audit'? Voldoen aan auditrechten wordt onderhandelen.

Concentratierisico is sectorbreed

Vier frontier-providers bedienen bijna de hele markt. Eén storing of verandering in gedrag raakt alle afnemers tegelijk.

Stoppen bij GenAI is in de praktijk bijna onmogelijk

Prompts, embeddings, fijnafstellingen en integraties zijn niet zomaar mee te nemen. 'Stoppen' betekent in feite: opnieuw bouwen.

Drie regimes — één praktische boodschap

Van brede ICT-dienst onder DORA / NIS2 naar smalle materiële uitbesteding onder sector-richtlijnen — de naam ('tool', 'licentie') is niet bepalend, de aard van de dienst wél

DORA — ICT-DIENST

Art. 3(21) DORA — bewust breed bedoeld

- Elke derde partij die ICT-diensten levert — of het nu 'tool', 'SaaS' of 'licentie' heet
- Foundation-model-API's, Copilot, AI-onderdelen in SaaS — vallen er standaard onder
- ICT-TP-register, beoordeling van materialiteit, vereisten in het contract
- Zwaarder regime voor 'kritieke of belangrijke' functies — meldplicht, exit-strategie, audit

Drempel: laag — bijna altijd van toepassing

EBA / EIOPA — UITBESTEDING

EBA GL/2019/02, EIOPA Cloud GL, DNB Q&A Uitbesteding

- Uitbesteding als een derde een functie van bank of verzekeraar ondersteunt of overneemt
- DNB: de naam ('licentie', 'abonnement') is niet bepalend — de aard van de dienst wél
- Cloud-levering van foundation-models voldoet meestal aan deze toets
- De EBA-richtlijnen worden in 2026 vervangen — AI/ICT-diensten vallen onder DORA / NIS2, niet-ICT onder de nieuwe richtlijn

Drempel: middel — de toets is of het een functie ondersteunt

MATERIËLE UITBESTEDING

Zwaarste regime: speelt bij kritieke of belangrijke functies

- Krediet, KYC/AML, claims, premiebepaling, handel — kernprocessen
- Vooraf melden bij DNB, contract voor uitbesteding, exit-plan, toets op concentratie
- De eindverantwoordelijkheid blijft bij de instelling — altijd, ongeacht de leverancier
- DNB jan 2026: ~21% van AI komt van derden — hier geldt dit regime zonder discussie

Drempel: hoog — maar speelt bij veel AI in de financiële sector

Vraag voor de zaal: pak één AI-toepassing binnen je eigen organisatie waar het regime tot nu toe 'licht' is aangepakt. Onder welk van deze drie regimes valt hij echt — en kun je dat juridisch verdedigen tegenover DNB, of hoop je stilletjes dat de vraag niet komt?

AIA, FRIA, DPIA — drie beoordelingen, één dossier

Vaak apart uitgevoerd, vaak dubbel werk. De kunst: één gezamenlijke beoordeling, drie uitkomsten.

AIA

AI Impact Assessment

Regel uit sector of huis

REIKWIJDTE

Wat doet het systeem, welke beperkingen, welke risico's — breed bedoeld

W A N N E E R

Bij elke AI-toepassing (licht voor minimaal, zwaar voor hoog-risico)

E I G E N A A R

Product + 2e lijn

FRIA

Fundamental Rights Impact Assessment

AI-Act art. 27

REIKWIJDTE

Effect op grondrechten: gelijke behandeling, privacy, vrijheid, toegang tot diensten

W A N N E E R

Verplicht voor hoog-risico deployers in publieke én deels private sector

E I G E N A A R

Compliance + Legal

DPIA

Data Protection Impact Assessment

AVG art. 35

REIKWIJDTE

Risico voor betrokkenen bij verwerking van persoonsgegevens — alléén persoonsgegevens

W A N N E E R

Hoog risico voor rechten en vrijheden (bij AI bijna altijd)

E I G E N A A R

Privacy Officer / FG

Praktijk: de drie overlappen voor ~60-70%. Één gecombineerde beoordeling met drie uitkomsten spaart dubbel werk en voorkomt inconsistente conclusies over hetzelfde systeem.

Opzet, bestaan, werking — toegepast op AI

De klassieke driedeling van audits blijft leidend. Op 'werking' gaan organisaties meestal de mist in.

OPZET

Zijn de juiste controles en bewijsmiddelen ingericht?

- Is er een AI-register en een sjabloon?
- Is er een crosswalk tussen eis en bewijs?
- Is er een sjabloon voor datasheet en model card?
- Ligt er een plan voor logging en bewaarbeleid?

Ontwerp op orde

BESTAAN

Zijn die onderdelen er echt en zijn ze ingevuld?

- Staan álle systemen in het AI-register?
- Zijn datasheets en model cards bijgewerkt?
- Zijn er screenshots van de kanaal-matrix?
- Staan bewijsstukken op de afgesproken plek?

Documentatie aanwezig

WERKING

Werkt het systeem ook in de praktijk?

- Worden reviews gedaan — en vastgelegd?
- Zijn logs op te vragen voor willekeurige gevallen?
- Worden CAPA's opgevolgd — met zichtbaar effect?
- Leeft het register — inclusief pilots en proeven?

Het werkt

Op 'werking' vallen organisaties meestal door de mand — het sjabloon bestaat, maar is niet bijgewerkt. De logging is bedacht, maar niet helemaal aangezet. Het register bestaat, maar mist pilots.

Vier stappen — een ritme dat steeds terugkomt

Geen project met begin en einde, maar een werkwijze die zich steeds herhaalt per AI-systeem

01	DoR <i>Definition of Ready</i> <i>Mogen we starten?</i>	Doel, doelgroep, aanpak van data, aanpak van fairness, uitleg, mens-in-de-lus en waar nodig AIA/FRIA/DPIA zijn vastgelegd. Afspraken over open-AI-gebruik liggen er.	<i>Zonder vastlegging geen meting.</i>
02	DoD <i>Definition of Done</i> <i>Is het echt af?</i>	Metingen op fairness en tests afgerond. Labels en B1-uitleg zichtbaar. Logging en bewaartermijn werken. Datasheet en model card bijgewerkt. Eerdere CAPA's gesloten.	<i>Zonder: het werk is vanuit bestuurlijk oogpunt niet opgeleverd.</i>
03	Review <i>Bewijsvergadering</i> <i>Zien we bewijs, of verhalen?</i>	Cijfers voor fairness, drift en prestaties. Voorbeelden uit het logboek. Afwijkingen uit het log. Labels zoals gebruikers die zien. Klachten en de CAPA's die erbij horen.	<i>Zonder: geen aantoonbare sturing.</i>
04	CAPA <i>Corrective & Preventive Actions</i> <i>Wordt er geleerd?</i>	Wat ging mis en waarom. Welke maatregel om te herstellen én om herhaling te voorkomen. Welk effect is zichtbaar. Tweede lijn bevestigt sluiting.	<i>Zonder: open CAPA's stapelen op — en toezichhouders tellen ze.</i>

Art. 13, 14, 50 — de zichtbare plichten in één oogopslag

Waar de toezichthouder op gaat testen: wat de gebruiker ziet, niet wat het beleid zegt

Art. 50 AI-ACT

Labels

Elk kanaal moet tonen dat AI meedoet.

RODE VLAG

Weinig labels; woorden verschillen per kanaal.

Snelle test: Trek één willekeurige klantbrief. Staat het erin?

Art. 13 AI-ACT

Uitlegbaarheid

Taal op B1-niveau, concrete redenen, zichtbare manier om bezwaar te maken.

RODE VLAG

Vakjargon; 'technische' uitleg; bezwaar verstopt.

Snelle test: Lees één uitleg zoals de klant die krijgt. Begrijp je het?

Art. 14 AI-ACT

Mens-in-de-lus

Medewerker ziet uitkomst, heeft tijd en bevoegdheid, afwijken wordt gelogd.

RODE VLAG

Override-KPI = 0% of juist heel hoog.

Snelle test: Laat drie overrides zien — met reden en uitkomst.

Recht op uitleg — van label naar verweer

Transparantie is meer dan een AI-label: de betrokkene moet het besluit kunnen begrijpen, controleren en aanvechten

0 1

Algemene uitleg

Vooraf, voor iedereen

Wat het systeem doet, het belang en de verwachte gevolgen, en welke rechten de betrokkene heeft — in gelaagde, op de doelgroep geteste taal.

0 2

Persoonlijke uitleg

Op verzoek, over dít besluit

Welke gegevens en afgeleide gegevens (zoals een risicoscore) zijn gebruikt en hoe de logica in dit geval tot de uitkomst leidde. Een formule alleen is onvoldoende.

0 3

Rechten & verweer

Vindbaar, begrijpelijk, effectief

Menselijke tussenkomst, standpunt kenbaar maken en het besluit aanvechten, plus klacht bij de AP of beroep bij de rechter. Niet alleen een bezwaarknop.

Het verband: *uitlegbaarheid is een ontwerpkeuze (explainability-by-design), niet een tekstlaag achteraf — en de uitleg is bewijs in de reviewset.*

Agentic AI — beheers de route, niet alleen de output

Een agent geeft geen antwoord, hij zet stappen — fouten verspreiden zich door de keten

0 1

Wat is anders

Niet de zin, maar de weg ernaartoe

Een agent plant en handelt: doel → plan → bron → tool → tussenstap → actie. Je beheerst de hele route, niet één antwoord.

0 2

Nieuwe controls

Waarmee houd je grip?

Agent-card, tool-permission matrix, vaste control points, state-log en een geteste kill switch. Geen onomkeerbare actie zonder mens.

0 3

Bewijs in de Review

Wat laat je zien?

Een echte agent-run: gebruikte bronnen, tussenstappen, menselijke ingrepen en een replay-test die de route herleidbaar maakt.

Het verband: *dezelfde governance als de rest — agent-controls horen in het register, de agent-run is het bewijs in de reviewset.*

Toezicht na livegang — waar governance echt wordt getest

Alleen testen vooraf is aantoonbaar onvoldoende. Dit is waar je het verschil maakt.

0 1

Logging

Kunnen we elke beslissing terughalen?

- Invoer en uitkomst van het model
- Modelversie op het moment van het besluit
- Elk moment waarop een mens afwijkt
- Fouten en incidenten

Test: iemand maakt bezwaar — kunnen we precies terugzien wat er gebeurde?

0 3

Incidenten

Worden signalen opgepakt?

- Kleurcodering rood/oranje/groen
- Oorzaak zoeken, niet alleen het probleem aanpakken
- Elk incident gekoppeld aan een CAPA
- Terugblik of de maatregel werkt

Test: welke incidenten kwamen terug? Dan werkte de CAPA niet.

0 2

Monitoring

Zien we patronen, niet alleen incidenten?

- fairness per groep — trendlijn
- Drift-signalen met drempels
- Klachten en bezwaren — aantal en soort
- Override-KPI — verloop in de tijd

Test: laat drie recente meldingen zien — én wat we ermee deden.

0 4

CAPA

Wordt er aantoonbaar geleerd?

- Wat ging mis — en waarom
- Maatregel om te herstellen én om herhaling te voorkomen
- Aantoonbaar effect (minder incidenten, betere fairness)
- Tweede lijn bevestigt sluiting

Test: is het effect te meten, of is alleen op uitzonderingen gestuurd?

BIA voor AI — welk systeem is écht kritiek?

Niet elk AI-systeem verdient hetzelfde gewicht. Zonder BIA wordt elk incident een verrassing voor het bestuur.

WAT JE PER AI-SYSTEEM VASTLEGT IN DE BIA

Hoe kritiek is het proces	In welk kernproces draait dit AI-systeem — klantwerving, krediet, claims, KYC, handel?
Afhankelijkheid	Is AI ondersteunend, doorslaggevend, of het proces zélf? Hoe groot is de stap terug naar handmatig?
RTO	Recovery Time Objective — hoe snel moet het weer op minimaal niveau draaien?
RPO	Recovery Point Objective — hoeveel verlies van recente data (prompts, embeddings, fijnafstellingen) is acceptabel?
MTPD	Maximum Tolerable Period of Disruption — wanneer wordt de schade onaanvaardbaar?
Terugvalplan	Handmatig proces, ander model, andere leverancier, of gecontroleerd stopzetten?
Effect op klanten	Wat merkt een klant bij 4u / 24u / 1 week uitval? Wat bij een fout AI-besluit?
Effect op de toezichthouder	Meldplicht DORA/NIS2? Speelt FRIA hier? Risico op publicatie?

DE UITKOMST — INDELING

Kritiek

RTO < 4u, terugvaloptie verplicht getest, 24/7 monitoring, directe opschaling naar crisisteam

Belangrijk

RTO 4-24u, terugvaloptie beschikbaar maar niet altijd getest, monitoring tijdens werkdagen

Ondersteunend

RTO > 24u, praktische terugvaloptie, lichte monitoring, gebruikers accepteren uitval

Zonder BIA: elk incident wordt een verrassing voor het bestuur. **Mét BIA:** indeling in kritiek / belangrijk / ondersteunend — en herstel dat past bij de klasse.

Ketencontinuïteit voor AI — de les van de mismatch

De klassieke BCM-les: het BCP-uur staat haaks op het SLA-uur van de leverancier. Bij AI speelt hetzelfde — alleen zwaarder.

HOE DE MISMATCH ER VAN BINNEN UITZIET

VOORBEELD | EEN FINANCIËLE INSTELLING

In het BCP voor het kredietproces staat: **RTO van 4 uur** bij uitval van het AI-risicomodel. De externe modelleverancier heeft in het contract: **SLA van 48 uur** bij ernstige incidenten. Niemand in de lijn kende deze afspraak. Het crisisteam bereikte de leverancier pas na anderhalve dag.

WAT GING ER MIS

- De RTO in het BCP was niet afgestemd op de afspraken met de leverancier
- De leverancier werd pas laat betrokken bij de opschaling
- Niemand wist wie contactpersoon was of welke afspraken golden
- De uitvoering ging ervan uit dat 'het geregeld was'

WAT JE PER KRITIEKE AI-LEVERANCIER VASTLEGT

Afgestemde RTO	De SLA van de leverancier sluit aan op jouw BCP — getoetst en bevestigd
Terugvaloptie	Ander model, handmatig proces of andere leverancier — aanwezig én getest
Aanspreekpunt	Naam + mobiel + opschaling — geen support-ticket-loket
Onderaanneming	Weet je wie jouw leverancier inschakelt? Frontier-provider onderaan?
Testverplichting	Doet de leverancier mee aan je BCM-oefening? Staat dat in het contract?
ISAE / assurance	Toegang tot ISAE 3402 / SOC-rapportages over de beheersing van de AI-dienst?
Model-update meldplicht	Hoe en wanneer meldt de leverancier een wezenlijke wijziging (art. 25)?

De les: afhankelijkheid verdwijnt niet door uit te besteden — het wordt pas beheersbaar als het zichtbaar, besproken en getest is.

Three Lines model — vertaald naar AI

Dezelfde lijnen, maar met taken en bewijsplichten die specifiek voor AI gelden

1 e LIJN

Business / Deployer

Werkt met AI en levert het bewijs

TAKEN

- Compleet dossier per systeem
- DoR/DoD, datasheet, model card
- Metingen op fairness, logging, incidenten
- CAPA's doorvoeren en effect aantonen

Levert op: Evidence-set per sprint of kwartaal

2 e LIJN

Risk / Compliance

Duidt, toetst, daagt uit — neemt niet over

TAKEN

- AIA/FRIA/DPIA-review
- Drempels voor fairness, labels, HITL
- Art. 25-besluiten
- Reviews van keten en leveranciers

Levert op: Onafhankelijk oordeel en advies aan board

3 e LIJN

Internal Audit

Spiegelt onafhankelijk — ziet de patronen

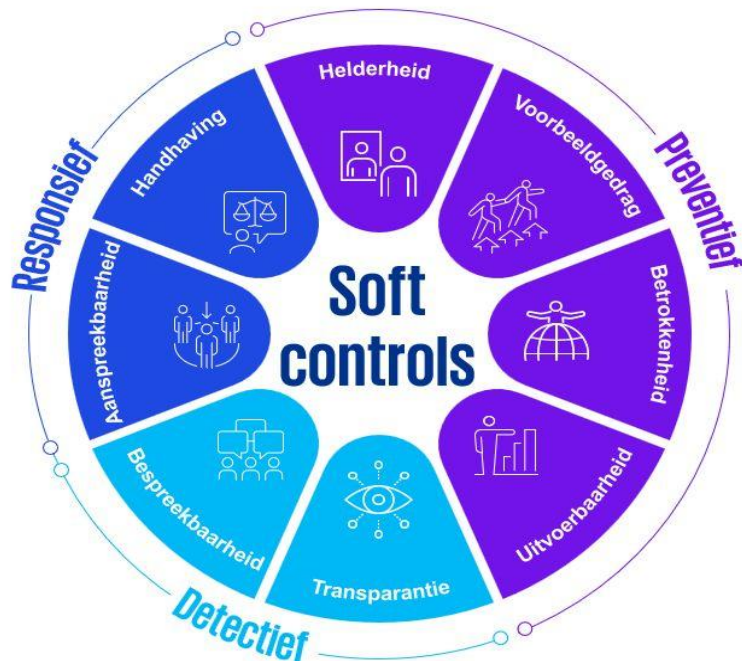
TAKEN

- Toetst of afspraken worden nageleefd
- Patronen in incidenten, drift, fairness
- Controleert of dossiers te herleiden zijn
- Rapporteerde aan RvC/auditcommissie

Levert op: Jaarlijks assurance-oordeel

Soft controls — waar harde governance op leunt

Hard controls leveren bewijs; soft controls bepalen of dat bewijs ook klopt met de praktijk



Naar het soft controls model van Muel Kaptein

Preventief — helderheid, voorbeeldgedrag, betrokkenheid, uitvoerbaarheid

De toets vooraf: weet de medewerker wat ‘goed AI-gebruik’ concreet betekent in zijn rol, geeft het management dat zelf zichtbaar het voorbeeld, en is het ook praktisch haalbaar binnen de werkdruk?

AI-test: heeft de claim-behandelaar 90 seconden of 9 minuten om af te wijken van het AI-advies? Zonder uitvoerbaarheid wordt HITL papieren controle.

Detectief — transparantie, bespreekbaarheid

De signalering tijdens: zien collega's wat AI doet (transparantie), en durven zij ‘dit klopt niet’ te zeggen tegen het model en tegen elkaar (bespreekbaarheid)?

AI-test: wordt ‘het model zegt het’ geaccepteerd als argument, of wordt het uitgedaagd? De override-KPI uit de reviewset meet dit indirect.

Responsief — aanspreekbaarheid, handhaving

De respons na: worden mensen aangesproken op AI-fouten zonder dat het in afrekenen verzandt, en wordt er ook echt gehandeld — CAPA met effect, niet alleen genoteerd?

AI-test: komen dezelfde incidenten terug? Dan werkte de CAPA niet — precies de testvraag uit het toezicht na livegang.

Doorkijk naar de stoplicht-check: het domein ‘Gedrag’ uit de zes domeinen op de volgende slide is precies de optelsom van deze acht soft controls.

Tien AI-risico's — de vaste checklist voor risicomangers

WERKVLOER · wat check je

BESTUUR · wat meld je

BESLUITTAFEL · wat vraag je

01	Fairness <i>Grote verschillen tussen groepen</i>	fairness-rapport per doelgroep; drempels + CAPA	02	Drift <i>Model verschuift ongemerkt</i>	Drift-dashboard met meldingen en CAPA als de drempel wordt overschreden
03	Onterecht besluit zonder mens <i>AI beslist in feite zelfstandig (art. 22 AVG)</i>	Snelle scan op besluit zonder mens; AIA/FRIA/DPIA; manier om bezwaar te maken	04	Schijn-zekerheid <i>Override-KPI = 0% of juist heel hoog</i>	Besliskaarten, override-log, training, bevoegdheid
05	Keten <i>Onduidelijke rollen, geen auditrechten</i>	Ketenmatrix; bepalingen in het contract; reviews op vaste momenten	06	Open-AI-misbruik <i>Vertrouwelijke prompts zonder logging</i>	Open-AI-log met 0 vertrouwelijke prompts; beleid
07	Incidenten <i>Klachten die terugkomen, open CAPA's</i>	Incidentlog met kleurcodes; CAPA- overzicht; trends	08	Datakwaliteit <i>Scheve data; AI-teksten als 'brondata'</i>	Datasheet; analyse op representativiteit; datakwaliteit
09	Rolverwarring <i>Wezenlijke wijziging (art. 25)</i>	Art. 25-besluit; bijgewerkt AI-register; crosswalk	10	BCM <i>Geen terugvaloptie bij uitval</i>	BCM-scenario's; kaart met terugvalopties; geteste uitwijk

Waar staan we nu — de stoplicht-check voor het bestuur

WERKVLOER · wat check je



BESTUUR · wat meld je



BESLUITTAFEL · wat vraag je

ZES DOMEINEN

Proces	Werken teams zichtbaar volgens DoR → DoD → Review → CAPA?
Data	Zijn kwaliteit, representativiteit en documentatie van data aantoonbaar?
Monitoring	Zien we drift, fairness, klachten en afwijkingen in dashboards — en wordt erop gehandeld?
Open-AI	Is het gebruik veilig, gelogd en volgens beleid (0 vertrouwelijke prompts)?
Keten	Zijn leveranciersafspraken duidelijk — auditrechten, art. 25, BCM?
Gedrag	Houden teams, tweede lijn en audit zich aan de afspraken? Melden mensen fouten zonder angst?

DE VERSIE VOOR HET BESTUUR



Rood — Basis ontbreekt

Onvolledige dossiers, geen trends in dashboard, onduidelijke rollen, geen zicht op keten of open-AI.



Oranje — Aanpak staat, maar nog niet stabiel

DoR/DoD wisselend ingevuld, overzicht deels op orde, monitoring niet volledig, CAPA's sluiten langzaam.



Groen — Volwassen & aantoonbaar

Vast ritme, duidelijke rollen, volledig bewijs, trends zichtbaar, keten en BCM goed geregeld.

Het gaat niet om 'alles groen'. Het gaat om weten waar de gaps zitten en gericht werken aan verbetering.

Drie vragen die bij élk AI-dossier op tafel horen

WERKVLOER · wat check je



BESTUUR · wat meld je



BESLUITTAFEL · wat vraag je

01

Welke rol hebben wij bij deze toepassing?

Aanbieder, deployer, importeur, distributeur — of een combinatie. De rol bepaalt welke plichten onder de AI-Act gelden en op welk niveau het toezicht wordt ingericht.

02

In welke risicoklasse valt dit systeem, en waarom?

Verboden, hoog, beperkt of minimaal — met onderbouwing en vastgelegd. Let op: bij hoog-risico is de volledige bewijsset verplicht, niet optioneel.

03

Welk bewijs zien we uit AI-register en review-evidence-set?

Geen verhalen, maar cijfers, logvoorbeelden, afwijkingen, CAPA's en voorbeelden van labels. Ontbreekt één? Dan is het systeem niet klaar voor audit.

Kun je één van deze drie vragen niet met bewijs beantwoorden? Dan is het dossier niet klaar voor besluitvorming of toezicht.

Wat dit vraagt — per rol aan tafel

Dezelfde drie ankers, vier verschillende invalshoeken

2 e LIJN

Tweede lijn

- Toetsingskader en indeling van risico's
- Drempels voor fairness en KRI's voor monitoring
- Regie op art. 25 bij wijzigingen
- Ketenreview met auditrechten

Onafhankelijk uitdagen van dossiers

3 e LIJN

Derde lijn

- Audit trail en bewijs
- Onafhankelijke toets op controles
- Analyse van patronen over systemen heen
- Assurance-oordeel richting RvC

Herleidbaarheid en patronen

CONSULTANT

Adviseur / consultant

- Ontwerp van controles en inrichting van het process DORA / NIS2
- Vertaling van AI-Act, en privacy naar beleid
- Invoeren van DoR/DoD/Review/CAPA
- Coaching van 1e en 2e lijn

Werkwijze en vertaling

BESTUUR / RvC

Bestuur en RvC

- Prioriteiten, risicobereidheid, toepassingen
- Verantwoordelijkheid en stuurinformatie
- De drie vaste vragen bij elk dossier
- Cultuur: fouten melden zonder angst

Richting, ritme en bewijs

De drie conclusies van deze bijeenkomst

0 1

Van experiment naar kernproces

AI komt steeds dichterbij besluitvorming en klantuitkomsten. Governance moet meegroeien — van een onderwerp aan de zijkant naar een onderwerp voor de hele onderneming. De literatuur in het AI Safety Report 2026 maakt dit onvermijdelijk.

0 2

Vier regimes, één systeem

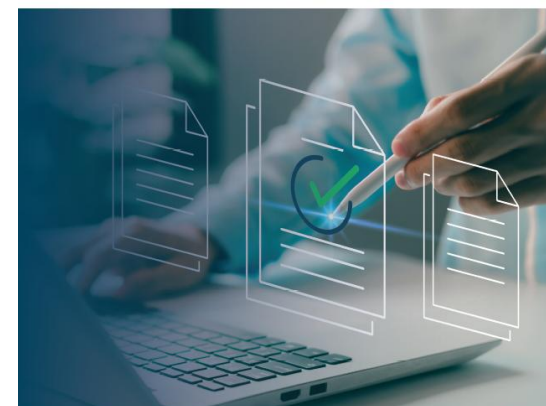
AI-Act, DORA / NIS2, AVG en aanbestedingsbeleid raken elkaar in bijna elke AI-toepassing. Wie ze apart beheert, betaalt vier keer en krijgt drie keer de verkeerde uitkomst. Toezichthouders kijken naar de samenhang.

0 3

Geen basis, geen bovenbouw

AI-register en review-evidence-set zijn de basis. AFM, DNB en audit gaan testen op bewijs, niet op bedoeling. Wat je niet kunt aantonen, kun je niet auditen — en dus ook niet verantwoorden.

*De winnaars zijn niet de instellingen die AI het snelst invoeren, **maar degenen die AI geloofwaardig, verantwoord en aantoonbaar in control kunnen inzetten.***



AI Governance in de Praktijk

Het complete handboek voor veilige, uitlegbare en eerlijke
AI in organisaties. Dé gids voor organisaties, bestuurders,
managers en teams.

Hein van den Steenhoven  **RCAAS**
AUDIT | RISK | COMPLIANCE | GOVERNANCE

EINDE / VRAGEN
