

AI Body of Knowledge

AI-BOK v1.3 – september 2026

Het referentiekader voor AI-governance, lifecycle management en organisatie-inrichting
13 kennisgebieden · 22 rollen · 22 faalmodi · 9 jurisdicties · open ArchiMate-model



Jan Willem van Veen · Principal Enterprise Architect
ISO 42001 · NIST AI RMF · EU AI Act · DAMA-DMBOK · TOGAF 10 · 2026

Inhoudsopgave

Wat de AI-BOK is	4
Waarom de AI-BOK	4
Wat v1.3 verandert	4
Waar te beginnen	5
Hoe bij te dragen	5
Voorwoord	5
Module 1: Kennisgebieden	6
Inleiding	6
Overzicht van de dertien kennisgebieden	6
KG1: AI Governance	8
KG2: AI Strategie & Portfoliomanagement	15
KG3: AI Architectuur	21
KG4: AI Lifecycle Management	29
KG5: Data & Semantiek voor AI	34
KG6: Modelmanagement	42
KG7: AI Interactie & Gebruikerservaring	51
KG8: AI Operations (AIOps/MLOps/LLMOps)	57
KG9: AI Risicomanagement & Veiligheid	63
KG10: AI Compliance & Audit	70
KG11: AI Ethiek & Verantwoord AI	75
KG12: AI Kennis- & Contextmanagement	81
KG13: AI-Geletterdheid & Capability Development	87
Module 2: Rollenmodel	92
2.0 Inleiding	92
2.1 Rollenoverzicht	92
2.2 Rolbeschrijvingen	93
2.3 RACI-model	114
2.4 Functiescheiding	117
2.5 Governance-structuur	119
2.6 Schaalbaarheid van het rollenmodel	123

2.7 Mapping naar EU AI Act-rollen	125
2.8 Samenvatting en samenhang	125
Module 3: Integratiemodule	127
3.0 Inleiding	127
3.1 AI Lifecycle Model	127
3.2 Meta-model	138
3.3 Governance-integratiemodel	144
3.4 Volwassenheidsmodel	160
3.5 Implementatieroadmap	171
3.6 Cognition Plane als integratielaag	178
3.7 AI-kwaliteitsraamwerk (cross-cutting)	198
3.8 Rol-gebaseerde leespaden en Minimum Viable Governance (MVG)	202
3.9 Slotwoord: de AI-BOK als samenhangend geheel	207
Bijlagen	208
Bijlage A: Worked examples per kennisgebied	209
Bijlage B: End-to-end agentic case (CHRA-v2)	213
Bijlage C: Brownfield-integratiegids	220
Bijlage D: MKB-playbook	224
Bijlage E: Templates en Checklists	228
Bijlage F: Begrippenlijst	241
Bijlage G: Bronnenlijst	247

AI-BOK Executive Summary - v1.3 (september 2026)

Een samenvatting van één pagina voor bestuurders, directie en senior stakeholders: wat de AI-BOK is, waarom hij bestaat, wat er in deze versie verandert, waar je begint en hoe je bijdraagt.

Wat de AI-BOK is

De AI Body of Knowledge (AI-BOK) is een open referentiekader voor AI-management: hoe een organisatie AI-systemen verantwoord bestuurt, bouwt, opereert, beveiligt en buiten gebruik stelt. Het bundelt een kennisstructuur, een rollenmodel, een integratiemodel, een volwassenheidsmodel, een open ArchiMate-referentie en een regelgevingstraceerbaarheidslaag tot één samenhangend geheel, vergelijkbaar met wat DAMA-DMBOK is voor datamanagement en TOGAF voor enterprise-architectuur. Het kader is open gelicentieerd, verschijnt in versie-releases en is bruikbaar voor organisaties van 50 FTE tot een wereldwijde onderneming.

Component	Aantal	Wat het is
Kennisgebieden	13	KG1 Governance (centraal) plus twaalf gebieden voor strategie, architectuur, lifecycle, data, modellen, interactie, operations, risico, compliance, ethiek, kennis en geletterdheid
Rollen	22	Strategisch, tactisch, operationeel en cross-functioneel, met een RACI van 22 rollen bij 13 kennisgebieden
Lifecycle-fasen	8	Ideatie & Verkenning tot en met Evolutie & Decommissioning, met vier feedbackloops
Metamodel-entiteiten	10	AI System, AI Model, Dataset, Prompt, Interactie, Beslissing, Kennisbron, Agent, Governance Framework, Risicoprofiel
Architectuurvlakken	4	Data plane, control plane, cognitievlak en management plane
Faalmodi	22	FM01-FM16 agentic en FM17-FM22 cyber-physical, elk met mechanisme, signatuur, detectie en mitigatie
Volwassenheidsniveaus	5	L1 Initieel tot L5 Geoptimaliseerd, met een bewijsrubric per kennisgebied

Waarom de AI-BOK

Geen bestaand instrument levert het geïntegreerde operating model dat een organisatie nodig heeft. ISO/IEC 42001 beschrijft managementprocessen zonder de vakinhoud die ze moeten dragen. NIST AI RMF benoemt risico's zonder eigenaren. De EU AI Act legt plichten op zonder te zeggen hoe een organisatie die belegt. De AI-BOK verbindt die drie: elk kennisgebied heeft een eindverantwoordelijke rol, elke plicht een plek in de lifecycle en elk risico een controle met bewijs.

Wat v1.3 verandert

v1.3 is een consistentie- en adoptierelease. Er komt geen kennisgebied bij; het kader wordt kloppend gemaakt en krijgt twee rollen die in de praktijk ontbraken.

- Twee adoptierollen.** De AI-Ambassadeur (Rol 21) draagt de adoptie binnen een team of afdeling; de AI-Specialist Prompting en Agents (Rol 22) beheert prompts, agentconfiguraties en de promptbibliotheek.
- RACI gecorrigeerd.** In eerdere versies hadden zeven van de dertien kennisgebieden geen eindverantwoordelijke. Elk kennisgebied heeft nu precies één A en minimaal één R; een validatiescript bewaakt dit.
- Vier architectuurvlakken.** Het management plane staat naast data plane, control plane en cognitievlak, in lijn met het peer-reviewed paper en het open ArchiMate-model.
- Consistentietooling.** Boek, ArchiMate-model en SemanticXL-pack lezen dezelfde canonieke bron; validatiescripts controleren rollen, niveaus, vlakken en de NL/EN-pariteit bij elke build.

Waar te beginnen

Begin met de **MVG-zeven** (Minimum Viable Governance, Module 3 §3.8): een governance charter, een AI-inventaris, een risicoclassificatie per systeem, lifecycle-gates, AI-geletterdheid met bewijs, compliance-traceerbaarheid en een incident-pipeline. Dat is een verdedigbare baseline voor elke organisatie, ook met vier gecombineerde rollen. Kies daarna het **leespad voor jouw rol** (Module 3 §3.8) en gebruik de worked examples in de bijlagen als de vorm van bewijs waar je naartoe werkt.

Hoe bij te dragen

De AI-BOK is een levend document. Voorstellen en correcties lopen via het reviewprotocol en de changelog op <https://www.ai-bok.nl>; releases tot nu toe: v1.0 (maart 2026), v1.1 (juni 2026), v1.2 (juni 2026) en v1.3 (september 2026). De regelgevingstraceerbaarheidsmatrix wordt elk half jaar gereviewd, het volwassenheidsmodel jaarlijks.

Feedback bij info@ai-bok.nl. Het open ArchiMate-model en de volledige documentenset zijn vrij te downloaden via <https://www.ai-bok.nl/architecture>.

Voorwoord

Ik werk al meer dan vijftientwintig jaar als architect. Eerst aan klassieke informatiesystemen bij de overheid, later aan dataplatformen en kennistechnologie en de afgelopen jaren steeds vaker aan AI. Wat begon als een specialisatie is iets geworden waar elke organisatie nu mee te maken heeft.

In mijn werk kom ik steeds hetzelfde patroon tegen. Een organisatie wil iets met AI. Iemand zoekt een raamwerk. ISO 42001 dekt het managementsysteem af, NIST schrijft over risico's, de AI Act bepaalt het wettelijk kader, maar samen vormen ze geen werkbaar geheel. Een AI-architect die wil weten hoe een agent zich verhoudt tot het cognitievlak moet zelf de puzzel leggen. Een risicomanager die zoekt naar de te verwachten faalmodi loopt vast op gefragmenteerde literatuur. Dat puzzelen kost veel tijd en gaat regelmatig fout.

Vandaar dit boek.

De AI Body of Knowledge brengt samen wat bestaande kaders niet zelf bieden: kennisgebieden, rollen, een levenscyclus, een metamodel, een volwassenheidsmodel en een referentiearchitectuur, in samenhang. Het is geen academisch werk en geen verzameling best practices. Het is een werkdokument voor mensen die maandagochtend verder moeten.

Mijn vakgebied is altijd betekenis geweest: semantische webtechnologie, knowledge graphs, linked data. Vanuit dat perspectief is mijn overtuiging dat betrouwbare AI niet ontstaat door betere modellen alleen. Ze ontstaat door betere betekenis: precieze begrippen, vertrouwde bronnen, expliciete kaders waarbinnen redenering plaatsvindt. Het cognitievlak vat dat samen als architectuurconcept.

In deze release (september 2026) staan de Nederlandse en Engelse uitgave op gelijke voet; de pariteit die in de vorige release werd hersteld is doorgetrokken naar alle modules. Het rollenmodel telt nu 22 rollen: naast kennisgebied 13 (AI-Geletterdheid) en rol 20 (Geletterdheidsfunctionaris) zijn rol 21 (AI-Ambassadeur) en rol 22 (AI-Specialist Prompting en Agents) opgenomen in de canonieke modules. De referentiearchitectuur werkt met vier vlakken: data plane, control plane, cognitievlak en management plane. De RACI-matrix is gecorrigeerd, onder meer voor de scheiding tussen de AI Auditor en de AI Compliance Officer. De consistentie tussen modules, rollenmodel en het SemanticXL-pack wordt bewaakt met geautomatiseerde validatie. De faalmodi-catalogus telt 22 patronen. Regelgevingstraceerbaarheid bestrijkt negen jurisdicties. De openbare referentiearchitectuur en alle bijbehorende ArchiMate-bestanden zijn te downloaden via <https://www.ai-bok.nl/architecture>.

Veel leesplezier.

Jan Willem van Veen · Principal Enterprise Architect · september 2026

Module 1: Kennisgebieden

Inleiding

De AI Body of Knowledge (AI-BOK) biedt een gestructureerd referentiekader voor organisaties die kunstmatige intelligentie op verantwoorde, architectureel onderbouwde en bestuurbare wijze willen inzetten. Module 1 definieert dertien kennisgebieden die samen het volledige domein van AI-management bestrijken, van strategie tot operatie, van ethiek tot architectuur en van compliance tot AI-geletterdheid.

De structuur is bewust gemodelleerd naar de kennisgebieden van DAMA-DMBOK, waarin Data Governance als centraal verbindend gebied fungeert. In de AI-BOK vervult **AI Governance** die rol: het overkoepelende kennisgebied dat richting geeft aan alle overige gebieden en waarborgt dat AI-initiatieven aansluiten bij organisatiedoelen, wet- en regelgeving en maatschappelijke verwachtingen.

Een onderscheidend concept binnen deze AI-BOK is het **cognitievlak** (cognition plane): de architectuurlaag waarin AI-systemen redeneren, interpreteren en beslissingen voorbereiden. Dit vlak vormt een aanvulling op de klassieke architectuurlagen (business, data, applicatie, technologie) en maakt expliciet zichtbaar waar autonome intelligentie opereert binnen de enterprise-architectuur.

Waarom een AI-BOK?

Een terechte tegenwerping is dat de fragmentatie in AI-governance ook zonder nieuw referentiekader oplosbaar zou moeten zijn: implementeer de bestaande standaarden gewoon beter, beleg de verantwoordelijkheden strakker, breng de architectuurpraktijk op orde. Elk van die remedies veronderstelt echter wat geen enkel bestaand instrument levert: een afgesproken inhoudsstructuur die zegt welke kennis een AI-functie moet onderhouden, wie daarvoor verantwoordelijk is en hoe de instrumenten zich tot elkaar verhouden. ISO/IEC 42001 eist processen maar beschrijft hun inhoud niet; het NIST AI RMF benoemt risico's maar geen eigenaren; de EU AI Act legt plichten op maar geen operating model. Organisaties die deze instrumenten combineren, moeten de integratie zelf construeren. Die integratie wordt in de praktijk telkens opnieuw en telkens anders gebouwd. De AI-BOK codificeert die integratie eenmalig: de kennisgebieden leveren de inhoudsstructuur, het rollenmodel de verantwoordelijkheden en de integratiematrix van Module 3 de expliciete verbindingen met ISO 42001, NIST AI RMF, EU AI Act, TOGAF en DAMA-DMBOK.

Notitie. Kennisgebied 13 - **AI-Geletterdheid & Capability Development** - verankert EU AI Act Artikel 4 (van kracht februari 2025) en geeft AI-geletterdheid een structureel huis naast de overige kennisgebieden. De cross-references vanuit KG1, KG3, KG9, KG10, KG11 en KG12 worden in de bijbehorende addenda (regelgevingskruistabel, volwassenheidsrubric, faalmodus-catalogus, leespaden, MVG-profiel, VNG/BZK/GEMMA-kruistabellen en het operationele/cyber-physical addendum) uitgewerkt.

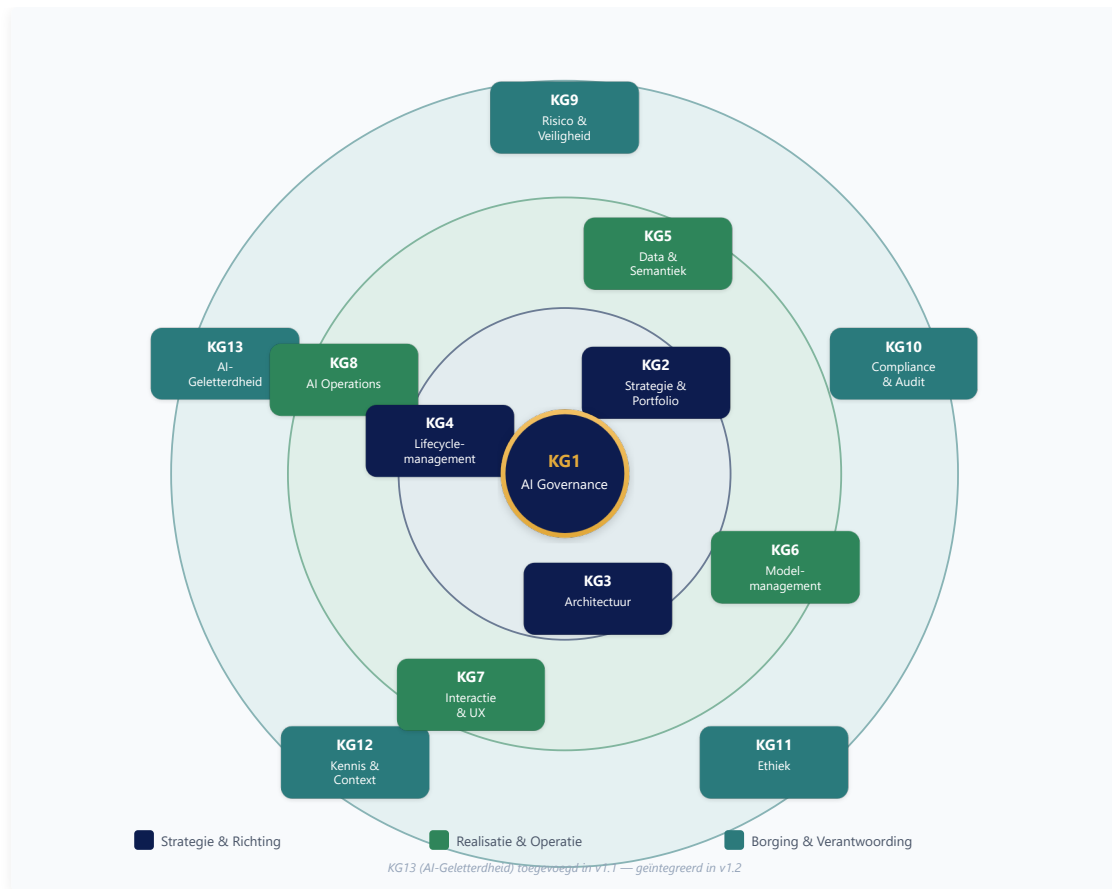
Status en doorontwikkeling

De AI-BOK is een **kandidaat-referentiekader**. De autoriteit van een body of knowledge ontstaat niet bij eerste publicatie maar door meerjarige, community-gedreven curatie, zoals DAMA-DMBOK die over meerdere edities heeft opgebouwd. Deze uitgave is hoofdzakelijk door één auteur geconstrueerd en in drie evaluatie-iteraties getoetst (practitioner-panel, onafhankelijk academisch expertpanel, pilottoepassingen); dat is een startpunt, geen eindstation. De validatie-roadmap loopt via samenwerking met praktijkcommunities (waaronder DANW en de FGEA Community of Practice), verbreding van het academische reviewpanel en longitudinaal onderzoek naar effectiviteit in organisaties. Lezers die willen bijdragen (correcties, praktijkervaringen, wijzigingsvoorstellen) kunnen dat doen via de kanalen op www.ai-bok.nl; daar staan ook het wijzigingslogboek en de gepubliceerde reviewprotocollen. Feedback wordt per release verwerkt en herleidbaar verantwoord.

Overzicht van de dertien kennisgebieden

Het onderstaande diagram toont de structuur van de AI-BOK. AI Governance vormt het centrale knooppunt; de overige twaalf kennisgebieden zijn gegroepeerd in drie ringen: Strategie & Richting, Realisatie & Operatie en Borging & Verantwoording.

(Zie Figuur 1: AI-BOK Framework - 13 kennisgebieden)



Figuur 1: AI-BOK Framework – 13 kennisgebieden

Leeswijzer: AI Governance staat centraal en is verbonden met alle overige kennisgebieden. De drie ringen geven de primaire oriëntatie aan:

- **Strategie & Richting** (2, 3, 4): Bepalen wat, waarom en hoe AI wordt ingezet
- **Realisatie & Operatie** (5, 6, 7, 8): Bouwen, trainen, deployen en opereren van AI-systemen
- **Borging & Verantwoording** (9, 10, 11, 12, 13): Waarborgen dat AI veilig, compliant, ethisch en betrouwbaar functioneert, met KG13 als de menselijke capability die de andere vier kennisgebieden operationeel maakt

KG1: AI Governance

1.1 Definitie

AI Governance omvat het geheel van besturingsstructuren, beleidslijnen, besluitvormingsprocessen en verantwoordingsmechanismen die waarborgen dat kunstmatige intelligentie binnen een organisatie doelgericht, verantwoord en beheerst wordt ontwikkeld, ingezet en uitgefaseerd. Het is het centrale en overkoepelende kennisgebied van de AI-BOK - vergelijkbaar met de rol die Data Governance speelt in DAMA-DMBOK. AI Governance bestrijkt nadrukkelijk ook het cognitievlak: de architectuurlaag waarin AI-systemen autonoom redeneren, interpreteren en handelen.

1.2 Doel en principes

Het doel van AI Governance is het scheppen van de voorwaarden waaronder AI-systemen maximale waarde leveren binnen aanvaardbare risicogrenzen. Daarbij gelden de volgende principes:

1. **Verantwoordelijkheid is expliciet belegd** - Voor elk AI-systeem is een eigenaar aangewezen die verantwoordelijk is voor het functioneren, de impact en de naleving van beleid. Verantwoordelijkheid mag niet impliciet blijven of verdeeld raken over functies zonder duidelijk mandaat.
2. **Besturing is proportioneel aan het risico** - De mate van governance-intensiteit is evenredig aan de risicoclassificatie van het AI-systeem. Een chatbot voor interne FAQ's vereist lichtere besturing dan een autonoom beslissysteem voor vergunningverlening. De EU AI Act-risicoclassificatie biedt hiervoor een bruikbaar referentiekader.
3. **Transparantie over autonomie** - De mate waarin een AI-systeem autonoom opereert, is vastgelegd en zichtbaar. Voor AI-agents betekent dit: expliciete documentatie van bevoegdheidsniveaus, contextgrenzen en escalatiedrempels.
4. **Governance is ingebed, niet opgelegd** - Governance-mechanismen zijn onderdeel van de AI-architectuur en het ontwikkelproces, niet een achteraf toegevoegde controlelaag. Policies worden bij voorkeur machine-leesbaar vastgelegd zodat agents ze runtime kunnen raadplegen.
5. **Menselijke controle als ontwerpprincipe** - Bij beslissingen met significante impact is human-in-the-loop of human-on-the-loop ingebouwd. Het escalatieniveau is per type beslissing vastgelegd in de governance-architectuur.
6. **Continue verbetering op basis van meetgegevens** - Governance is niet statisch. Op basis van monitoring, incidenten en volwassenheidsassessments worden besturingsstructuren periodiek bijgesteld.

1.3 Scope

Valt binnen scope:

- Vaststelling van AI-beleid, -principes en -richtlijnen op organisatieniveau
- Inrichting van besturingsorganen (AI Board, AI Review Committee, AI Ethiekcommissie, optioneel een AI Center of Excellence)
- Definitie en toewijzing van rollen en verantwoordelijkheden conform RACI
- Besluitvormingskaders voor AI-initiatieven, inclusief go/no-go-criteria en dispensatieprocedures
- Governance van het cognitievlak: besturing van de laag waarin AI-agents redeneren en handelen
- Naleving van interne standaarden en externe regelgeving (EU AI Act, ISO 42001)
- Koppeling met enterprise governance, IT governance en data governance
- Bestuurlijke escalatie- en incidentmechanismen

Valt buiten scope:

- Operationele uitvoering van risicomanagement (zie KG9)
- Technische implementatie van compliance-controles (zie KG10)
- Formulering van de AI-strategie zelf (zie KG2)

- Architectuurontwerp en -beheer (zie KG3)

1.4 Kernactiviteiten

1. **Vaststellen van het AI-governance-raamwerk** - Ontwerpen en formaliseren van de besturingsstructuur inclusief mandaten, bevoegdheden en besluitvormingslijnen. Het raamwerk positioneert AI Governance ten opzichte van bestaande corporate governance, IT governance en data governance. ISO 42001 biedt een bruikbare basis voor de structuur van het managementsysteem.
2. **Ontwikkelen van AI-beleid en -principes** - Formuleren van organisatiebrede beleidslijnen die de kaders stellen voor verantwoorde AI-inzet. Dit omvat beleid voor datagebruik door AI, transparantie, menselijke controle, non-discriminatie en duurzaamheid. De OECD AI Principles en de vereisten uit de EU AI Act dienen als vertrekpunt.
3. **Inrichten van AI-besturingsorganen** - Opzetten van de benodigde gremia: een AI Board voor strategische besluitvorming, een AI Review Committee voor de tactische toetsing bij gates, een AI Ethiekcommissie voor ethische toetsing en, als organisatorische optie, een AI Center of Excellence voor kennisdeling en standaardisatie. De samenstelling en mandaten worden afgestemd op de omvang en het volwassenheidsniveau van de organisatie.
4. **Classificeren van AI-systemen naar risico** - Elk AI-systeem wordt ingedeeld in een risicocategorie op basis van de EU AI Act (onaanvaardbaar, hoog, beperkt, minimaal) en aanvullende organisatiespecifieke criteria. De classificatie bepaalt de governance-intensiteit en de verplichte maatregelen.
5. **Definiëren van rollen en verantwoordelijkheden** - Toewijzen van eigenaarschap per AI-systeem, model en dataset. De RACI-matrix specificeert wie verantwoordelijk, aansprakelijk, geconsulteerd en geïnformeerd is. Dit omvat zowel menselijke rollen als gedefinieerde verantwoordelijkheden voor AI-agents zelf (mandaten, grenzen).
6. **Besturen van agent-autonomie** - Vaststellen van bevoegdheidsniveaus voor AI-agents, van volledig menselijke controle tot gedelegeerde autonomie. Per agent wordt vastgelegd: welk domein, welke bronnen, welke acties, welke escalatiedrempels. Dit is een specifieke governance-uitdaging van het cognitievlak.
7. **Beheren van agent-identiteiten** - AI-agents zijn non-human identities (NHI's) die dezelfde identity governance vereisen als menselijke gebruikers. Dit omvat vijf capabilities: (1) *discovery en classificatie* - identificeer alle actieve agents in het landschap en classificeer ze naar risico en bevoegdheidsniveau, (2) *eigenaarschap* - wijs aan elke agent een menselijke eigenaar toe om orphaned agents en onbeheerd risico te voorkomen, (3) *lifecycle governance* - bestuur hoe agent-identiteiten worden aangemaakt, gewijzigd en uitgefaseerd om permission creep te voorkomen, (4) *observability* - koppel agentactiviteit aan toegangsrechten om verborgen risico's zichtbaar te maken en (5) *auditability* - borg herleidbaarheid en auditgereed bewijs. Naarmate het aantal agents in productie groeit, wordt identity governance voor NHI's een voorwaarde om het AI-landschap beheersbaar te houden.
8. **Monitoren van AI-volwassenheid** - Periodiek beoordelen van de organisatiebrede AI-volwassenheid aan de hand van het AI-BOK-volwassenheidsmodel. Het assessment bestrijkt alle dertien kennisgebieden en levert een verbeterplan op.
9. **Coördineren van cross-functionele samenwerking** - Afstemming organiseren tussen business, IT, data, juridisch, compliance, ethiek en architectuur. AI-governance is per definitie multidisciplinair; geen enkele afdeling kan het alleen besturen.
10. **Behandelen van governance-incidenten** - Inrichten van een escalatie- en responsmechanisme voor AI-gerelateerde incidenten: ongewenste output, bias-detectie, beveiligingsinbreuken, compliance-schendingen. Het mechanisme omvat triage, onderzoek, mitigatie en rapportage.

11. **Rapporteren en verantwoorden** - Periodieke governance-rapportages opstellen voor directie, toezichthouders en relevante stakeholders. Rapportages omvatten governance-dekkingsgraad, incidenten, volwassenheidsontwikkeling en compliance-status.

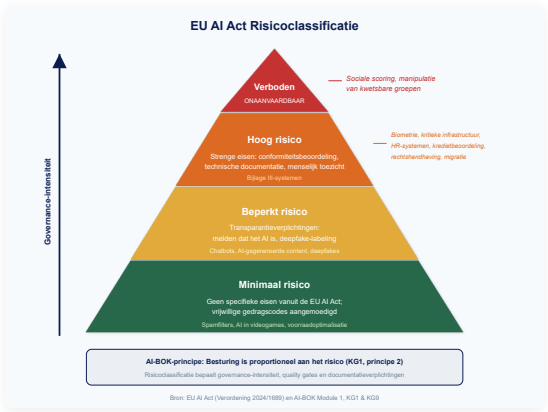
1.5 Rollen en verantwoordelijkheden

Rol	Verantwoordelijkheid	Referentie
Chief AI Officer (Rol 1)	Eindverantwoordelijk voor het AI-governance-raamwerk en de AI-strategie; voorzitter van het AI Board	Module 2, Rol 1
AI Board (orgaan)	Strategische besluitvorming over AI-beleid, risicoacceptatie, portfolioprioritering en het organisatiebrede maximum voor agent-autonomie	Module 2, §2.5
AI Governance Lead (Rol 7)	Ontwerpt en onderhoudt het governance-raamwerk en het beleid; secretaris van het AI Board en voorzitter van het AI Review Committee	Module 2, Rol 7
AI Product Owner (Rol 4)	Systeemeigenaar van een specifiek AI-systeem; verantwoordelijk voor classificatie, compliance en prestaties; als gebruiksverantwoordelijke eigenaar van DPIA en FRIA	Module 2, Rol 4
AI Ethiek-adviseur (Rol 3)	Bewaakt ethische principes en adviseert over dilemma's; voorzitter van de AI Ethiekcommissie	Module 2, Rol 3
AI Agent-gouverneur (Rol 18)	Stelt per agent het autonominiveau vast binnen het door het AI Board bepaalde maximum en beheert het agentbevoegdheidsregister	Module 2, Rol 18
AI Compliance Officer (Rol 19)	Coördineert en voert compliance-assessments uit, waaronder DPIA en FRIA; eindverantwoordelijk voor KG10	Module 2, Rol 19
Functionaris gegevensbescherming (FG; extern aan het rollenmodel)	Adviseert over de AVG-naleving van AI-systemen die persoonsgegevens verwerken (art. 39 AVG); adviseert en keurt niet goed	Extern aan het rollenmodel

1.6 Technieken en hulpmiddelen

- AI Governance Framework Canvas
- Visueel hulpmiddel om de besturingsstructuur te ontwerpen en te communiceren
- RACI-matrix
- Vastlegging van rollen en verantwoordelijkheden per AI-systeem
- AI-risicoclassificatiemodel
- Gestructureerde methode om AI-systemen in te delen naar risicoprofielen (conform EU AI Act) *(Zie Figuur 2: EU AI Act risicoclassificatie)*

- Volwassenheidsmodel (AI-BOK CMM)
- Beoordelingsraamwerk op vijf niveaus voor alle dertien kennisgebieden
- Policy-as-code tooling
- Machine-leesbare vastlegging van governance-regels (bijv. Open Policy Agent, Rego) zodat AI-agents runtime beleidsregels kunnen raadplegen
- Governance-tooling / enterprise-architectuurtool
- Vastlegging van governance-structuren, mandaten en agentbevoegdheden als architectuurartefacten
- AI-governance-dashboard
- Real-time overzicht van governance-dekkingsgraad, incidenten en compliance-status



Figuur 2: EU AI Act risicoclassificatie

1.7 Inputs en outputs

Inputs:

- Enterprise-strategie en -governance-kaders

- Wet- en regelgeving (EU AI Act, AVG, sectorspecifieke regulering)
- AI-volwassenheidsassessment (nulmeting)
- Risico-inventarisatie uit KG9 (AI Risicomanagement)
- Architectuurprincipes uit KG3 (AI Architectuur)
- Incidentrapportages en audit-bevindingen uit KG10

Outputs:

- AI Governance Charter
- AI-beleidsraamwerk en AI-principes
- RACI-matrix voor AI-rollen
- AI-risicoclassificatieregister
- AI-governance-dashboard en periodieke rapportages
- Mandaten en bevoegdheidskaders voor AI-agents
- Dispensatie- en escalatieprocedures

1.8 Implementatierichtlijnen

1. **Begin met een AI Governance Charter** - Stel een kort, gezaghebbend document op dat het mandaat, de scope en de bestuursorganen definieert. Laat dit goedkeuren door de raad van bestuur. Zonder formeel mandaat blijft AI Governance een adviesfunctie zonder doorzettingsmacht.
2. **Sluit aan bij bestaande governance-structuren** - Bouw AI Governance niet op als geïsoleerd silo. Integreer met IT governance (COBIT), data governance (DAMA-DMBOK) en enterprise-architectuur (TOGAF). Hergebruik bestaande gremia waar mogelijk en voeg AI-specifieke expertise toe.
3. **Maak governance proportioneel en gelaagd** - Definieer drie tot vier governance-niveaus gekoppeld aan risicoclassificatie. Vermijd one-size-fits-all; zware governance voor laagrisico-toepassingen remt innovatie, te lichte governance voor hoogrisicosystemen creëert aansprakelijkheidsrisico's.
4. **Investeer in policy-as-code** - Leg governance-regels vast in documenten en in machineleesbare vorm. In een architectuur met AI-agents moeten agents runtime hun bevoegdheden en beperkingen kunnen verifiëren zonder menselijke tussenkomst.

1.9 Governance-aspecten

AI Governance is zelf het governance-kennisgebied en dient als zodanig ook haar eigen besturing te organiseren:

Periodieke review

Het AI-governance-raamwerk wordt jaarlijks geëvalueerd op effectiviteit en relevantie, of vaker bij significante wijzigingen in wet- en regelgeving

Onafhankelijke toetsing

De interne auditfunctie of een externe partij toetst periodiek de werking van de governance-structuur (in samenhang met KG10)

Escalatiemechanisme

Bij conflicten tussen governance-eisen en operationele belangen escaleert het AI Board naar het bestuur

Wijzigingsbeheer

Aanpassingen in AI-beleid en -principes volgen een formeel wijzigingsproces met versioning en impactanalyse

1.10 Metrics en KPI's

#	Metric	Beschrijving	Streefwaarde	Meetfrequentie
1	Governance-dekkingsgraad	% AI-systemen onder formeel governance-toezicht	≥ 95%	Kwartaal
2	Beleidsnalevingspercentage	% AI-initiatieven conform vastgesteld AI-beleid	≥ 90%	Kwartaal
3	Risicoclassificatie-compleetheid	% AI-systemen met vastgestelde risicoclassificatie	100%	Maand
4	Time-to-decision	Mediaan doorlooptijd van governance-besluitvorming	≤ 10 werkdagen	Kwartaal
5	Volwassenheidsscore	Score op AI-BOK volwassenheidsmodel (1-5)	≥ 3 (jaar 1), ≥ 4 (jaar 3)	Halfjaar
6	Incidentresponstijd	Mediaan tijd tot mitigatie van governance-incidenten	≤ 48 uur	Maand
7	Agent-mandaat-dekkingsgraad	% operationele AI-agents met vastgelegd bevoegdheidskader	100%	Kwartaal
8	Agent-identiteit-dekkingsgraad	% AI-agents met geregistreerde NHI, menselijke eigenaar en actuele toegangsrechten	100%	Kwartaal
9	Orphaned-agent-ratio	% agents zonder actieve menselijke eigenaar	0%	Maand
10	Cross-governance-integratie	Aantal formele koppelingen met IT/data/enterprise governance	≥ 3 actieve koppelingen	Jaar

1.11 Relatie met andere kennisgebieden

KG2 (AI Strategie)

Governance stelt de kaders waarbinnen strategie wordt geformuleerd; strategie levert input voor governance-prioriteiten

KG3 (AI Architectuur)

Governance definieert architectuurprincipes; architectuur biedt de structuur om governance machine-leesbaar te implementeren

KG4 (AI Lifecycle Management)

Governance bepaalt de gate-criteria in elke fase van de levenscyclus

KG5 (Data & Semantiek)

Governance stelt eisen aan datakwaliteit en semantische precisie; begrippenkaders vormen het fundament voor eenduidige governance-definities

KG9 (AI Risicomanagement)

Governance stelt de risicotolerantie vast; risicomanagement levert input voor governance-beslissingen

KG10 (AI Compliance & Audit)

Governance mandateert compliance-eisen; audit toetst de werking van governance

KG11 (AI Ethiek)

Governance verankert ethische principes; ethiek adviseert over dilemma's die governance moet beslechten

KG12 (Kennis- & Contextmanagement)

Governance stelt eisen aan de betrouwbaarheid van kennisbronnen die agents als context gebruiken

1.12 Relevante standaarden

Standaard	Relevantie voor dit kennisgebied
ISO/IEC 42001:2023	AI Management System - biedt de structuur voor het governance-raamwerk
ISO/IEC 38507:2022	Governance implications of AI - richtlijnen voor bestuurlijke verantwoordelijkheid
EU AI Act (2024)	Wettelijke verplichtingen voor aanbieders en gebruiksverantwoordelijken, risicoclassificatie
NIST AI RMF 1.0	Govern-functie - best practices voor AI-governance

Standaard	Relevantie voor dit kennisgebied
OECD AI Principles	Vijf principes voor verantwoorde AI die als beleidsbasis dienen
ISO/IEC 23894:2023	AI Risk Management - aanvullend op governance-raamwerk
COBIT 2019	IT-governance-framework waarmee AI Governance moet integreren

Business rules en beslisstandaarden:

Standaard	Relevantie voor dit kennisgebied
DMN (Decision Model and Notation)	OMG-standaard voor het modelleren van beslissingen en beslisregels. Relevant voor AI-governance omdat het de formele specificatie biedt van de beslisregels die AI-systemen toepassen of ondersteunen. DMN maakt het mogelijk om menselijke en AI-beslissingen in dezelfde notatie vast te leggen, wat transparantie en auditeerbaarheid vergroot.
SBVR (Semantics of Business Vocabulary and Business Rules)	OMG-standaard voor het formaliseren van zakelijke vocabulaire en bedrijfsregels in gestructureerd natuurlijke taal. Relevant voor het vertalen van governance-beleid naar machineleesbare regels die door AI-systemen kunnen worden toegepast.
RuleML / SWRL	Standaarden voor het uitdrukken van regels bovenop RDF/OWL-ontologieën. Maken het mogelijk om governance-regels, compliance-vereisten en bedrijfslogica als formele regels vast te leggen die door AI-agents kunnen worden geraadpleegd en toegepast.

1.13 Shadow AI: onzichtbaar risico, zichtbare aanpak

Definitie. Shadow AI is het gebruik van AI-tools en -systemen door medewerkers zonder medeweten, goedkeuring of governance van de organisatie. Waar shadow-IT traditioneel gaat over ongeautoriseerde hardware en software, richt shadow AI zich specifiek op generatieve en analytische AI-diensten die medewerkers op eigen initiatief inzetten: ChatGPT voor het schrijven van e-mails en notities, GitHub Copilot voor code, Midjourney voor presentatievisualisaties, of zelfgebouwde GPT's voor data-analyse. Het onderscheidende kenmerk is dat de organisatie geen zicht heeft op welke data deze systemen verwerken, welke output ze genereren en welke afhankelijkheden ze creëren.

Omvang van het probleem. Een aanzienlijk deel van het AI-gebruik in organisaties valt buiten formele governance; vrijwel elke interne inventarisatie brengt meer tools aan het licht dan de IT-functie kent. Dit is geen randverschijnsel: in vrijwel elke afdeling, van marketing tot finance, van HR tot juridisch, experimenteren medewerkers met AI-tools om productiever te werken. De motivatie is begrijpelijk (sneller werken, betere output), maar het onbeheerste karakter maakt shadow AI tot een van de urgentste governance-uitdagingen. Het probleem verergert naarmate AI-functionaliteit wordt ingebed in bestaande tools (Microsoft 365 Copilot, Google Gemini in Workspace, Adobe Firefly) waardoor de grens tussen "gewoon gebruik" en "AI-gebruik" vervaagt.

Risico's. Shadow AI introduceert vijf categorieën risico die direct raken aan de governance-verantwoordelijkheid:

1. **Data-lekkage:** Medewerkers voeren bedrijfsgevoelige informatie in bij externe AI-modellen (klantgegevens, financiële data, strategische plannen). Deze data kan worden opgeslagen, gebruikt voor training of toegankelijk zijn voor derden.
2. **Compliance-schending:** Verwerking van persoonsgegevens door externe AI-diensten kan in strijd zijn met de AVG (geen verwerkingsovereenkomst, geen DPIA). Onder de EU AI Act kan ongecontroleerd gebruik van hoogrisico-AI-systemen leiden tot substantiele boetes.
3. **Inconsistente output:** Verschillende medewerkers gebruiken verschillende AI-tools met verschillende prompts, wat leidt tot inconsistente kwaliteit, tegenstrijdige adviezen en onherleidbare beslissingen.
4. **Reputatieschade:** AI-gegenereerde output die fouten bevat, bias vertoont of ongepast is, wordt naar buiten gebracht zonder review, met reputatieschade als gevolg.
5. **Oncontroleerbare afhankelijkheden:** Bedrijfsprocessen worden afhankelijk van externe AI-diensten zonder contractuele borging, SLA's of continuïteitsplanning. Wanneer een dienst wijzigt of stopt, vallen processen stil.

Detectie. Effectieve detectie van shadow AI vereist een combinatie van technische en organisatorische maatregelen:

- **Netwerk-monitoring op AI-API-verkeer:** Identificeer uitgaand verkeer naar bekende AI-endpoints (api.openai.com, generativelanguage.googleapis.com, etc.) via firewall-logs en proxy-analyse.
- **Software-inventarisatie:** Scan endpoints op geïnstalleerde AI-applicaties, browser-extensies en plugins die AI-functionaliteit bieden.
- **Medewerkerenquêtes:** Voer periodiek (minimaal halfjaarlijks) anonieme enquêtes uit waarin medewerkers worden gevraagd welke AI-tools zij gebruiken en waarvoor. Anonimiteit vergroot de kans op eerlijke antwoorden.

- **Browser-extensie-monitoring:** Monitor browser-extensies die AI-functionaliteit injecteren in webapplicaties.
- **API-gateway-analyse:** Analyseer uitgaande API-aanroepen op patronen die wijzen op AI-diensten (grote tekst-payloads, multimodale uploads).

Aanpak: kanaliseren, niet verbieden. Een verbod op AI-gebruik is contraproductief: medewerkers zullen workarounds vinden en de organisatie loopt innovatie mis. De effectieve aanpak is kanaliseren:

1. **Bied veilige alternatieven:** Stel enterprise-versies beschikbaar van populaire AI-tools (Azure OpenAI, AWS Bedrock) met data-verwerking binnen de organisatiegrenzen en verwerkingsovereenkomsten.
2. **Stel een AI-gebruiksbeleid op:** Definieer helder welke categorieën data wel en niet mogen worden ingevoerd in AI-systemen, welke use cases zijn toegestaan en welke goedkeuring vereisen.
3. **Creëer een "goedgekeurde tools"-lijst:** Publiceer en onderhoud een levende lijst van AI-tools die zijn beoordeeld op privacy, beveiliging en compliance. Maak het proces om een tool te laten beoordelen laagdrempelig (maximaal 2 weken doorlooptijd).
4. **Maak melden laagdrempelig:** Creëer een cultuur waarin medewerkers open kunnen delen welke AI-tools zij gebruiken, zonder angst voor sancties. Een "AI-gebruik meldpunt" of Slack-kanaal verlaagt de drempel.
5. **Train en bewustmaak:** Bied korte, praktische trainingen aan over verantwoord AI-gebruik, gericht op de risico's van onbeheerst gebruik en de beschikbare alternatieven.

Governance-integratie. Shadow AI-management integreert met meerdere kennisgebieden van de AI-BOK:

- De **shadow AI-inventarisatie** vormt directe input voor KG9 (Risicomanagement): elk onbeheerst AI-systeem is een risico dat moet worden beoordeeld, geclassificeerd en gemitigeerd.
- De compliance-implicaties worden beheerd via KG10 (AI Compliance & Audit): elk shadow AI-systeem moet worden getoetst aan AVG, EU AI Act en sectorspecifieke regelgeving.
- De technische aspecten (API-monitoring, enterprise-alternatieven) vallen onder KG3 (AI Architectuur) en KG8 (AI Operations).
- De culturele en organisatorische dimensie raakt aan KG13 (AI-Geletterdheid & Capability Development): het opbouwen van AI-geletterdheid, onder regie van de AI Geletterdheidsfunctionaris (Rol 20) en gedragen door de AI-Ambassadeurs (Rol 21), vermindert de neiging tot onbeheerst gebruik.

Gebruik **Template 5 (Shadow AI Inventarisatie)** als praktisch hulpmiddel om het huidige shadow AI-landschap in kaart te brengen en als basis voor het opstellen van een gericht actieplan. De inventarisatie moet periodiek worden herhaald (minimaal halfjaarlijks) omdat het AI-landschap snel evolueert.

Zo gaat het boek verder

Module 1: nog twaalf kennisgebieden, elk met activiteiten, rollen, metrics, standaarden en een relatie met DAMA-DMBOK, TOGAF, ISO 42001 en NIST AI RMF.

Module 2: het rollenmodel met 22 rollen, de RACI-matrix en functiescheiding.

Module 3: lifecycle, meta-model, volwassenheidsmodel, implementatieroadmap, het cognitievlak voor AI-agents en elf rol-gebaseerde leespaden.

Bijlagen: vijf templates, uitgewerkte voorbeelden, mkb-playbook en een end-to-end agentic case.

Bestellen: www.ai-bok.nl (39,95 euro inclusief btw, 255 pagina's).