REFERENTIEKADER

NEDERLANDSE EDITIE



AI Body of Knowledge

Governance, architectuur en organisatie van AI in één samenhangend kader

AI-BOK 1.6 · november 2026

13	22	27	4
KENNISGEBIEDEN	ROLLEN	FAALMODI	ARCHITECTUURVLAKKEN

Jan Willem van Veen
Principal Enterprise Architect

Aansluitend op EU AI Act · ISO/IEC 42001 · NIST AI RMF · TOGAF · DAMA-DMBOK

Inhoudsopgave

Wat de AI-BOK is 5
Waarom de AI-BOK 6
Wat v1.6 verandert 6
Waar te beginnen 6
Hoe bij te dragen 7
Gebruik en licenties 7

Voorwoord 8

Module 1: Kennisgebieden 9

Inleiding 9
Overzicht van de dertien kennisgebieden 11
KG1: AI Governance 13
KG2: AI Strategie & Portfoliomanagement 25
KG3: AI Architectuur 34
KG4: AI Lifecycle Management 47
KG5: Data & Semantiek voor AI 56
KG6: Modelmanagement 71
KG7: AI Interactie & Gebruikerservaring 87
KG8: AI Operations (AIOps/MLOps/LLMOps) 98
KG9: AI Risicomanagement & Veiligheid 110
KG10: AI Compliance & Audit 123
KG11: AI Ethiek & Verantwoord AI 134
KG12: AI Kennis- & Contextmanagement 143
KG13: AI-Geletterdheid & Capability Development 153

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

Module 2: Rollenmodel 163

2.0 Inleiding 163

2.1 Rollenoverzicht 164

2.2 Rolbeschrijvingen 167

2.3 RACI-model 214

2.4 Functiescheiding 217

2.5 Governance-structuur 221

2.6 Schaalbaarheid van het rollenmodel 226

2.7 Mapping naar EU AI Act-rollen 230

2.8 Samenvatting en samenhang 237

Module 3: Integratiemodule 238

3.0 Inleiding 238

3.1 AI Lifecycle Model 239

3.2 Meta-model 255

3.3 Governance-integratiemodel 264

3.4 Volwassenheidsmodel 294

3.5 Implementatieroadmap 311

3.6 Cognition Plane als integratielaag 322

3.7 AI-kwaliteitsraamwerk (cross-cutting) 363

3.8 Rol-gebaseerde leespaden en Minimum Viable Governance (MVG) 372

3.9 Slotwoord: de AI-BOK als samenhangend geheel 379

Bijlagen 380

Bijlage A: Worked examples per kennisgebied 381

Bijlage B: End-to-end agentic case (CHRA-v2) 387

Bijlage C: Brownfield-integratiegids 396

Bijlage D: MKB-playbook 405

Bijlage E: Templates en Checklists 414

Bijlage F: Begrippenlijst 450

Bijlage G: Bronnenlijst 466

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

AI-BOK Executive Summary v1.6 (november 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. Het wil voor AI-management worden wat DAMA-DMBOK is voor datamanagement en TOGAF voor enterprise-architectuur, maar is nu nog een kandidaat-referentiekader: opgesteld door één auteur, getoetst in drie evaluatierondes en open voor correctie door de praktijk. 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 vijf 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	**27**	FM01-FM16 en FM23-FM27 agentic, FM17-FM22 cyber-physical, elk met mechanisme, signatuur, detectie en mitigatie
Volwassenheidsniveaus	**5**	L1 Initieel tot L5 Geoptimaliseerd, met een bewijsrubric per kennisgebied
Kwaliteitsdimensies	**6**	Van datakwaliteit tot redeneer- en groundingkwaliteit, met metrics en streefwaarden per dimensie
Templates	**12**	Blanco werkinstrumenten in Bijlage E, gekoppeld aan de MVG-onderdelen

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

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 v1.6 verandert

Deze versie maakt het kader beter bruikbaar in de uitvoering. Er komen geen kennisgebieden, rollen of metamodelentiteiten bij; de levenscyclus krijgt een vijfde feedbackloop.

- **FRIA volgens het model van het AI-bureau.** Template 10 volgt de indeling van het concept dat het AI-bureau op 16 november 2026 ter consultatie publiceerde: een risicoblok per grondrecht met restrisico, het menselijk toezicht, de respons en een bewijsketen met triggers voor herbeoordeling. Het concept is nog niet vastgesteld; de template zegt dat ook.
- **De harness als stuurobject.** Uitkomsten hangen evenveel af van wat rond het model staat als van het model zelf. KG3 §3.14 beschrijft die harness, legt haar per release vast in een harnessmanifest en geeft vijf controls en criteria voor hervalidatie.
- **Beoordelen vóór handelen.** KG7 §7.13 beschrijft wat een beoordelaar doet voordat iemand op AI-output handelt: vier uitkomsten, drie niveaus van beoordelingsdiepte en een minimaal beoordelingsrecord. Zo is zinvol toezicht te onderscheiden van een formele klik.
- **Exposure management en uitzonderingen.** KG8 §8.14 koppelt de bestaande registers tot één beeld van de AI-aanvalsvlakken, zonder nieuw register. KG10 §10.14 onderscheidt bewijs van opzet en van werking en legt elke uitzondering vast met eigenaar, restrisico, compenserende maatregel en hersteltermijn.
- **Mandaatloop.** Een assurance-, audit- of incidentbevinding over een agent perkt het mandaat in tot de hervalidatie is afgerond (fase 7 naar fase 2, §3.1.0a).
- **Eén lijn in de besluitvorming.** Business case, faseovergang en dispensatie hebben nu overal dezelfde beslisser: het AI Review Committee bij de quality gates, het AI Board bij hoog risico en bij dispensatie. Kernrollen, rolcombinaties en scorecard-eigenaren volgen Module 2.
- **Actuele standaarden.** De MCP-revisie van juli 2026, de optionele ondertekening van A2A-agent cards, de OWASP Agent Control Standard en een incident uit de evaluatiepraktijk zijn verwerkt.

Waar te beginnen

Begin met de **MVG-zeven** (Minimum Viable Governance, Module 3 §3.8.2): 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. Wie al AI in productie heeft of in de publieke sector

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

werkt, kiest eerst het passende instapprofiel (§3.5.0); Bijlage E geeft per MVG-onderdeel het template. 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), v1.3 (september 2026), v1.4 (oktober 2026), v1.5 (november 2026) en v1.6 (november 2026). De regelgevingstraceerbaarheidsmatrix wordt elk half jaar gereviewd, het volwassenheidsmodel jaarlijks.

Open review. Elke minor release krijgt vooraf een commentaarperiode van zes weken. Reacties lopen via info@ai-bok.nl; elke reactie krijgt een nummer en een besluit (overgenomen, deels, niet overgenomen, met reden) in de changelog van de release. Externe reviewers worden met hun toestemming bij naam genoemd. Het doel is een vast panel van drie tot vijf reviewers uit architectuur, recht en audit.

Gebruik en licenties

- **Boek en toolkit:** gebruik volgens de licentievoorwaarden op ai-bok.nl (persoonlijk, team of organisatie). Korte citaten met bronvermelding zijn toegestaan.
- **Open delen:** AI-BOK Core (open data met vaste codes) valt onder CC BY 4.0. De ArchiMate-modellen staan in de openbare repository AI-thesaurus en vallen onder de licentie van die repository (GPL-3.0).
- **Tekst- en datamining:** voor het boek en de toolkit behoudt de auteur zich het recht op tekst- en datamining voor, ook voor het trainen van AI-modellen (artikel 4, lid 3, van Richtlijn (EU) 2019/790). Voor de open delen geldt hun eigen licentie.
- **AI-gebruik:** bij onderzoek, review en redactie van deze uitgave zijn AI-hulpmiddelen gebruikt. Alle inhoud is door de auteur beoordeeld en vastgesteld; de auteur is verantwoordelijk voor de tekst.
- **Geen juridisch advies:** de AI-BOK beschrijft de stand van het recht zorgvuldig, maar vervangt geen juridisch advies voor een concrete situatie.

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 vijfentwintig 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 werkdocument 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.

Deze release (november 2026) gaat over de uitvoering. Bij elke inzet van AI zag ik dezelfde vraag terugkomen: wat doet iemand op het moment dat hij op de uitvoer gaat handelen en wat ligt er rond het model dat het gedrag evenzeer bepaalt? Kennisgebied 3 beschrijft daarom de harness rond het model en kennisgebied 7 de beoordeling vóór het handelen. Kennisgebied 8 en 10 maken zichtbaar of een maatregel ook werkt en hoe je een uitzondering vastlegt. Template 10 volgt nu het concept van het AI-bureau voor de grondrechteneffectbeoordeling. De levenscyclus heeft een vijfde feedbackloop: een bevinding over een agent perkt het mandaat in tot hervalidatie. Verder staat overal dezelfde beslisser bij business case, faseovergang en dispensatie. Laat vooral weten waar het boek in de praktijk knelt. De openbare referentiearchitectuur, de ArchiMate-bestanden en de open data staan op https://www.ai-bok.nl/architecture.

Veel leesplezier.

Jan Willem van Veen · Principal Enterprise Architect · november 2026

Module 1: Kennisgebieden

Inleiding

Stand van het recht en labels. Deze module volgt de AI-verordening zoals gewijzigd door Verordening (EU) 2026/1744, stand 23 november 2026. De hoogrisicoverplichtingen gelden voor systemen van bijlage III vanaf 2 december 2027 en voor systemen van bijlage I vanaf 2 augustus 2028; de Nederlandse uitvoeringswet is nog een voorstel. Labels: Norm betekent een eis uit wet of geharmoniseerde norm, Modelkeuze een keuze van de AI-BOK, Advies een aanbeveling. In de gate-criteria en het MVG-profiel zijn criteria zonder label modelkeuzes.

> **IN HET KORT**
>
> **Wat:** Dertien kennisgebieden: wat een organisatie moet weten en doen om AI te besturen, te bouwen, te beheren en te verantwoorden.
>
> **Eigenaar:** Per kennisgebied één eindverantwoordelijke rol (RACI in Module 2).
>
> **Eerste stappen:** Begin met KG1, KG9, KG10 en KG13; die dragen het grootste deel van het MVG-profiel (Module 3, §3.8.2).
>
> **Wettelijke haak:** Per kennisgebied in dit blok; het overzicht staat in de regelgevingsmatrix (Module 3, §3.3.8).

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.

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

Elk kennisgebied sluit af met een blok **Eerste 90 dagen**: een startvolgorde voor een organisatie die met dat kennisgebied begint. De blokken sluiten aan op fase 1 van de implementatieroadmap (Module 3 §3.5.1) en verwijzen naar de templates in Bijlage E.

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 wélke kennis een AI-functie moet onderhouden, wíe daarvoor verantwoordelijk is en hóe 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 integratiematrices 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 toepassing sinds 2 februari 2025, herschreven door Verordening (EU) 2026/1744) en geeft AI-geletterdheid een structureel huis naast de overige kennisgebieden. De verbindingen met KG1, KG3, KG9, KG10, KG11 en KG12 staan in Module 3: regelgevingsmatrix (§3.3.8), sectorintegratie (§3.3.9), bewijsrubric (§3.4.9), faalmoduscatalogus (§3.6.7), operationele en cyber-physical AI (§3.6.8) en leespaden en MVG (§3.8).*

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.

Sinds versie 1.5 heeft elk object in het kader een vaste identificatiecode: `urn:aibok:KA9` voor kennisgebied 9, `urn:aibok:R18` voor rol 18, `urn:aibok:FM23` voor faalmodus 23, enzovoort. De codes zijn taalneutraal (KA staat voor KG) en worden nooit hergebruikt. Alle kennisgebieden, rollen, gremia, fasen, niveaus, MVG-onderdelen, faalmodi en metamodelentiteiten zijn met hun onderlinge

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

relaties en het RACI-raster ook als open data beschikbaar (AI-BOK Core, SKOS in JSON-LD en CSV, licentie CC BY 4.0) in de toolkit en naast de ArchiMate-modellen. Wie een eigen register, risicolog of architectuurmodel aan de AI-BOK koppelt, gebruikt die code als sleutel.

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.



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

KPI-streefwaarden. Elk kennisgebied sluit af met een tabel met KPI's in de sectie Metrics en KPI's. De streefwaarden daarin zijn indicatief. Ze komen uit de praktijkervaring achter dit boek en uit de kalibratietabellen in de toolkit, niet uit een norm of een vergelijkend onderzoek. Gebruik ze als

vertrekpunt: doe eerst een nulmeting, stel daarna per KPI een eigen streefwaarde vast en leg die vast in het AI-beleid (KG1). Waar een waarde wel een externe grond heeft, zoals de meldtermijnen van artikel 73 of de meetregels voor evaluaties in §6.14, staat dat bij de KPI zelf.

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

KG1: AI Governance

IN HET KORT

Wat: Het besturingskader voor alle AI: organen, beleid, besluitvorming en escalatie.

Eigenaar: Chief AI Officer (Rol 1), met de AI Governance Lead (Rol 7) als uitvoerder.

Eerste stappen: Inventariseer de AI in gebruik (Template 5), stel de charter vast (Template 1), classificeer elk systeem (Template 3).

Wettelijke haak: Geen eigen artikel; de inrichting draagt de plichten van aanbieder (art. 16 en 17) en gebruiksverantwoordelijke (art. 26).

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.

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

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

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

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. Leg daarbij ook het operating model vast: een centraal Center of Excellence dat de AI-inzet zelf uitvoert, een hub-

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

and-spoke-model waarin een centraal team strategie, standaarden en tooling levert en uitvoerende teams in de bedrijfsonderdelen werken, of een gefedereerd model waarin domeinen binnen centrale kaders zelf ontwikkelen. Hub-and-spoke wordt in de praktijk vaak als startvorm beschreven. De keuze bepaalt welke rollen uit Module 2 centraal zitten en welke in de lijn.

4. **Classificeren van AI-systemen naar risico:** Elk AI-systeem wordt ingedeeld in een risicocategorie op basis van de EU AI Act (verboden, hoog risico, transparantieplicht art. 50, overig) 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.

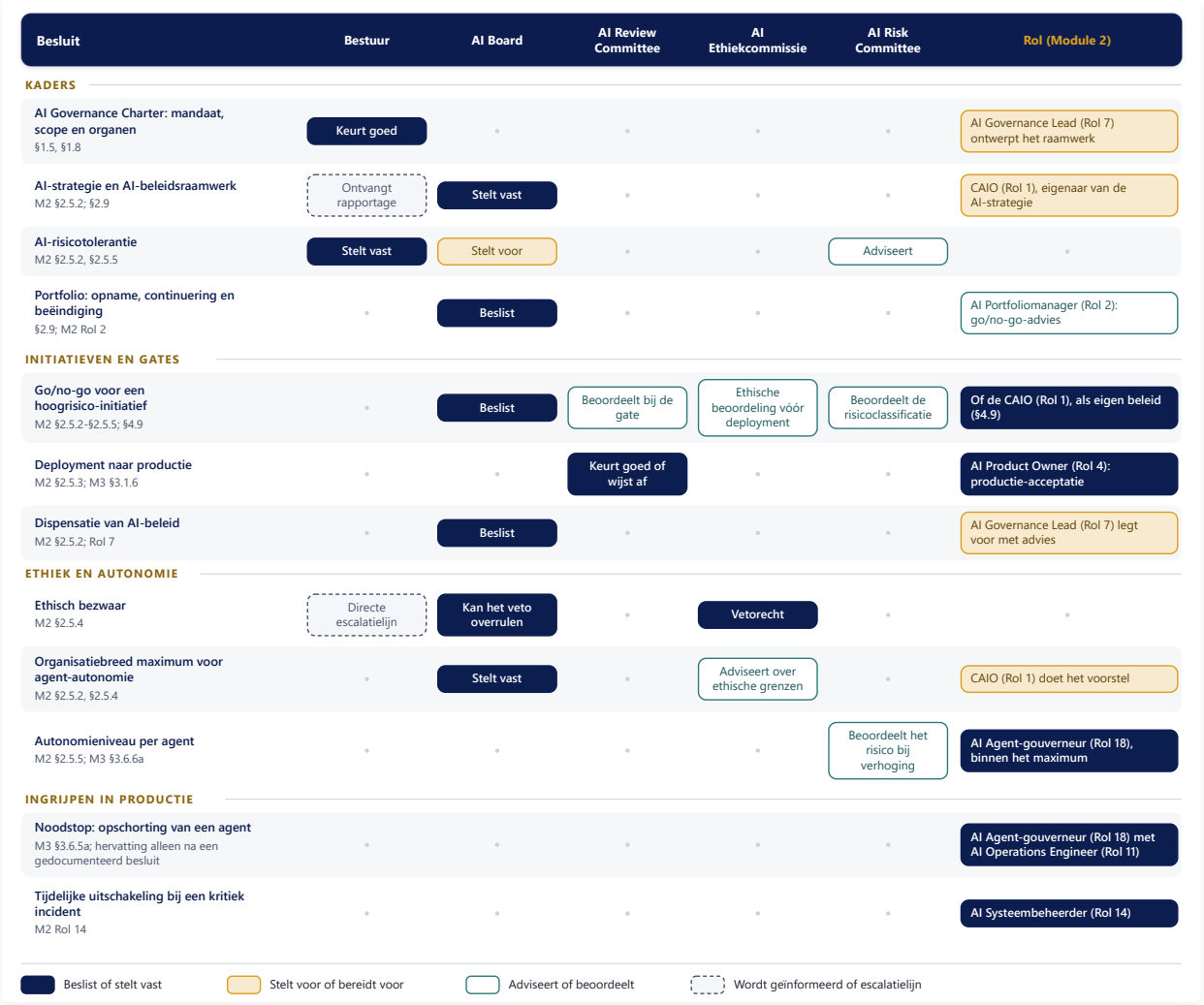
1.5 Rollen en verantwoordelijkheden

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

Rol	Verantwoordelijkheid binnen KG1
Chief AI Officer (Rol 1)	Eindverantwoordelijk voor het AI-governance-raamwerk en de AI-strategie; voorzitter van het AI Board
AI Board (orgaan)	Strategische besluitvorming over AI-beleid, risicoacceptatie, portfolioprioritering en het organisatiebrede maximum voor agent-autonomie
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
AI Product Owner (Rol 4)	Systeemeigenaar van een specifiek AI-systeem; verantwoordelijk voor classificatie, compliance en prestaties; namens de organisatie (verwerkingsverantwoordelijke en gebruiksverantwoordelijke) eindverantwoordelijk voor DPIA en FRIA
AI Ethiek-adviseur (Rol 3)	Bewaakt ethische principes en adviseert over dilemma's; voorzitter van de AI Ethiekcommissie
AI Agent-gouverneur (Rol 18)	Stelt per agent het autonomieniveau vast binnen het door het AI Board bepaalde maximum en beheert het agentbevoegdheidsregister
AI Compliance Officer (Rol 19)	Coördineert en voert compliance-assessments uit, waaronder DPIA en FRIA; eindverantwoordelijk voor KG10
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

De CAIO-rol is inmiddels gangbaar. In de IBM CEO Study 2026 (enquête onder 2.000 CEO's in 33 landen, mei 2026) meldt 76% van de organisaties een CAIO, tegen 26% een jaar eerder; die steekproef is scheef verdeeld naar grote organisaties. In de Amerikaanse federale overheid verplicht OMB-memorandum M-25-21 (april 2025) elk agentschap een CAIO aan te wijzen; een bestaande CIO, CDO of CTO met aantoonbare AI-expertise mag die rol vervullen.

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl



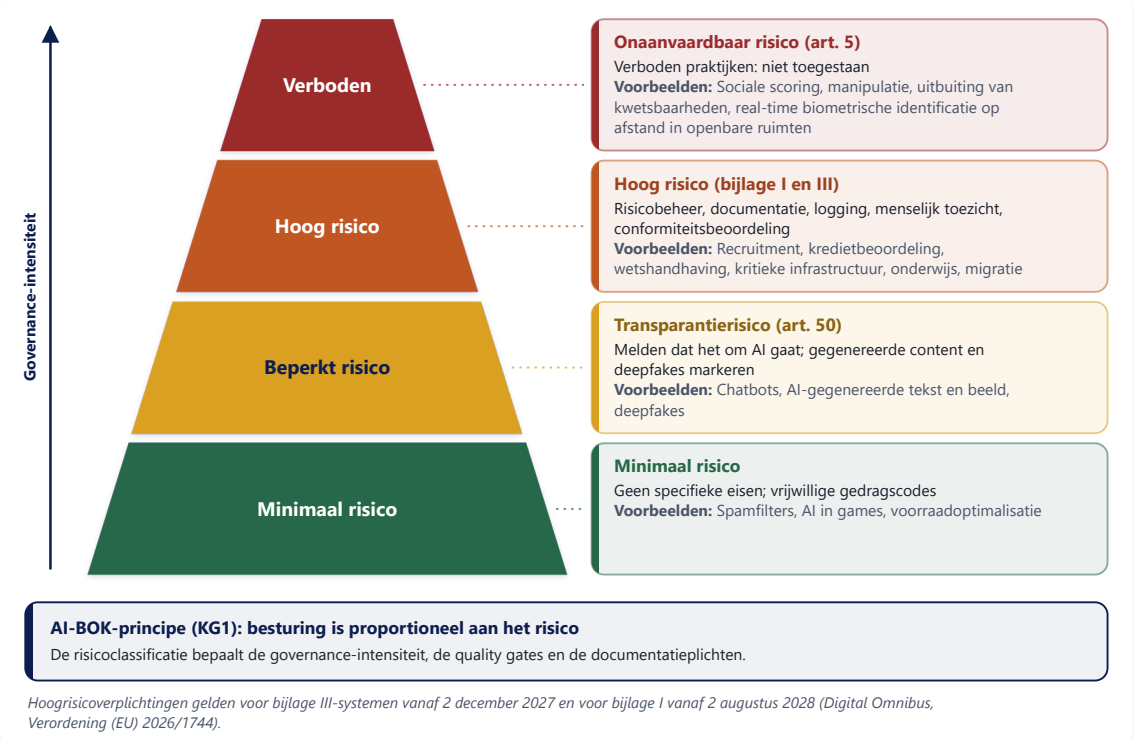
Figuur 2: Beslisrechten in AI-governance

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)
- **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

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

- **AI-governanceplatforms:** Sinds 2026 een eigen productcategorie (Gartner publiceerde in 2026 een eerste Magic Quadrant). Ze bundelen AI-inventaris, risicobeoordeling, beleidsregels en bewijs. Beoordeel ze op de objecten van dit kader: register, mandaat, beslissingsartefact en bewijs van werking



Figuur 3: 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

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

- 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 besturingsorganen 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.

Eerste 90 dagen

Startvolgorde voor een organisatie die met dit kennisgebied begint.

1. **Week 1-2:** Wijs een voorlopige AI Governance Lead (Rol 7) aan en breng met Template 5 (Shadow AI Inventarisatie) in kaart welke AI-toepassingen al in gebruik zijn.
2. **Week 3-4:** Stel met Template 1 (AI Governance Charter) het mandaat, de scope en de besturingsorganen op en leg de charter ter vaststelling voor aan het bestuur.
3. **Maand 2:** Classificeer de geïnventariseerde systemen met Template 3 (EU AI Act Compliance Checklist) en koppel per risicoklasse een governance-niveau (§1.8, richtlijn 3).
4. **Maand 2:** Wijs per AI-systeem een eigenaar aan en leg de toewijzing vast met de RACI-presentatie uit de AI-BOK Toolkit (ai-bok.nl/toolkit).
5. **Maand 3:** Registreer elk systeem in productie met Template 2 (AI-systeemregistratie) en leg voor elke agent in gebruik met Template 7 (Agentbevoegdheidsregister-vermelding) de non-human identity en de menselijke eigenaar vast; leg per verleend mandaat het besluit vast met Template 8 (Mandaatrecord).
6. **Dag 90:** Meet de uitgangssituatie met Template 4 (AI Volwassenheidsassessment) en rapporteer de eerste KPI's uit §1.10 aan het AI Board.

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

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

- **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

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

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

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

- **KG5 (Data & Semantiek):** Governance stelt eisen aan datakwaliteit en semantische precisie; begrippenkaders vormen het fundament voor eenduidige governance-definities
- **KG9 (AI Risicomanagement):** Governance bereidt de risicotolerantie voor die het bestuur vaststelt (Module 2, §2.5.2); 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; NIST werkt aan een herziening, versie 1.0 is nog de geldende
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; opvolger COBIT 7 is door ISACA aangekondigd voor 27 oktober 2026; COBIT 2019-certificaten blijven geldig (stand november 2026)
IEEE 2863-2026	Recommended Practice for Organizational Governance of AI (oktober 2026): aanvulling op de inrichting van het governance-raamwerk

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.

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

Standaard	Relevantie voor dit kennisgebied
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. Onderzoek bevestigt de omvang. In het MIT NANDA-rapport *The GenAI Divide* (juli 2025; 52 interviews en 153 enquêterespondenten) had 40% van de bedrijven een officieel LLM-abonnement afgesloten, terwijl medewerkers in ruim 90% van de bedrijven eigen AI-tools voor hun werk gebruikten. In de Microsoft Work Trend Index 2024 (31.000 kennismedewerkers; een leveranciersonderzoek) zei 78% van de AI-gebruikers eigen AI-tools mee te nemen naar het werk. Schaduwgebruik schuift daarnaast op van chattools naar agents en automatiseringen die medewerkers zelf bouwen met low-code-agentbouwers, eigen GPT's of agentische codeertools. Zulke agents hebben vaak eigen koppelingen en datatoegang en horen daarom in de inventarisatie en in het agentbevoegdheidsregister (Rol 18).

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 substantiële boetes.

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

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.
- **Medewerkersenquêtes:** 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 (bijvoorbeeld Microsoft Foundry met Azure OpenAI of Amazon 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 maak bewust:** Bied korte, praktische trainingen aan over verantwoord AI-gebruik, gericht op de risico's van onbeheerst gebruik en de beschikbare alternatieven.

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

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. Neem daarin ook door medewerkers gebouwde agents en automatiseringen op, met eigenaar, gebruikte tools en koppelingen en datatoegang. De inventarisatie moet periodiek worden herhaald (minimaal halfjaarlijks) omdat het AI-landschap snel evolueert.

Inkijkexemplaar van de AI Body of Knowledge v1.6. Het volledige boek: www.ai-bok.nl

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, 27 faalmodi en elf rol-gebaseerde leespaden.
Bijlagen: twaalf blanco templates, uitgewerkte voorbeelden, een mkb-playbook met gemeentelijke variant, een end-to-end agentic case en open data met vaste codes.

Bestellen: www.ai-bok.nl (485 pagina's).