BEST PRACTICE

BiSL en de Europese AI Act

Een praktijkgericht, auditbaar raamwerk voor verantwoord AI-gebruik binnen Business Informatiemanagement

Yvette Backer, Lex Scholten & René Visser

knvi Open Standards

bisl®

Colofon

Titel:	BiSL en de Europese AI Act *Een praktijkgericht, auditbaar raamwerk voor verantwoord AI-gebruik binnen Business Informatiemanagement* Versie / datum: 1.0 (12 juni 2026) Op basis van: BiSL® 4de editie (Van Haren) en Verordening (EU) 2024/1689 (AI Act)
Auteur(s):	Yvette Backer, Lex Scholten, René Visser
Reviewer(s):	Jasper Maas, Frank van Outvorst, Jacintha Hall, Raymond Swinkels
Contact KNVI:	KNVI Interessegroep Open Standaarden (open_standaarden@knvi.nl)

Deze whitepaper is tot stand gekomen met ondersteuning van AI-technologie. De inhoud is volledig beoordeeld en bewerkt door de auteurs.

Organisaties achter deze paper

Over KNVI

KNVI, de Koninklijke Nederlandse Vereniging van Informatieprofessionals, is in Nederland hét platform voor Professionals in Informatiemanagement, Informatietechnologie en Informatievoorziening, waar iedere professional in deze disciplines zich thuis voelt. Informatie speelt een leidende rol in de ontwikkeling van mens en maatschappij. Wij zien het dan ook als onze taak om de ontwikkeling van informatieprofessionals te bevorderen, door samen te werken, te faciliteren, elkaar te ontmoeten, focus aan te brengen en voorop te lopen. Daarbij houden we rekening met onze kernwaarden onafhankelijkheid, integriteit, professionaliteit.[1]

Over de interessegroep 'Open Standaarden'

Het doel van de interessegroep 'Open Standaarden' is om de professionals van KNVI te ondersteunen door een onafhankelijke verzameling van aanbevolen standaarden aan te bieden welke ook voldoen aan vooraf opgestelde criteria. Deze interessegroep sluit ook perfect aan op de overige interessegroepen omdat er standaarden van die onderwerpen in de lijst zullen staan zoals Architectuur, Beheer en Servicemanagement, Informatiemanagement, Governance etc. Daarnaast zijn de doelen van de interessegroep om:

- Het bijhouden van open standaarden door middel van een open en vrij toegankelijk online bibliotheek, waarbij iedere standaard gemaakt is op het 9-vlaksmodel.
- Het verbinden van Open Standaarden, door de toepassing en integratie van verschillende methoden te beschrijven en faciliteren.
- En het bijdrage aan verenigingsactiviteiten ten behoeve van Open Standaarden.

De ambitie van deze interessegroep is om het go-to punt te zijn voor professionals die op zoek zijn naar nieuwe standaarden in zijn of haar vakgebied maar goedgekeurd en aanbevolen door de KNVI.[2]

[1] https://www.knvi.nl/over-knvi
[2] https://www.knvi.nl/interessegroep/open-standaarden

Inhoudsopgave

Samenvatting (abstract)

De Europese AI Act introduceert een risico gebaseerd regime voor het ontwikkelen, in de handel brengen en gebruiken van AI-systemen. Voor organisaties die Artificiële Intelligentie (AI) inzetten als onderdeel van hun informatievoorziening verschuift “AI-compliance” van een eenmalige toets naar een structurele besturings- en beheervraag. Dit whitepaper verbindt de wettelijke eisen van de AI Act met het BiSL®-framework voor Business informatiemanagement (BIM). Het resultaat is een concreet en auditbaar handelingsperspectief: welke BiSL-processen leveren welke compliance-producten op, op welk moment in de AI-levenscyclus, en hoe worden risico’s en impact van gebruiksscenario’s aantoonbaar beheerst.

De kernbijdrage is een integrale werkwijze waarin (1) de afstemming tussen vraag en gebruik expliciet wordt gemaakt, (2) de AI Act-risicoklasse wordt vastgesteld, en (3) passende organisatorische, procesmatige en contractuele controles worden ingericht. Hiermee worden besluitvorming en verantwoording rond AI-inzet traceerbaar, herhaalbaar en toetsbaar, zowel voor de interne governance als voor externe toezichthouders.

Trefwoorden: BiSL, Business informatiemanagement, AI Act, compliance, risicobeheer, datagovernance, leveranciersmanagement, lifecyclemanagement, General Purpose AI (GPAI), bewijsvoeringsketen (evidence supply chain).

1. Inleiding en positionering

AI-systemen worden in organisaties in toenemende mate ingezet voor besluitvorming, ondersteuning van medewerkers, automatisering van informatieverwerking en interactie met klanten. Daarmee worden AI-componenten onderdeel van de informatievoorziening (IV) en vallen zij onder dezelfde besturingsvraagstukken als andere IV-middelen: wie is eigenaar, welk bedrijfsdoel wordt ondersteund, welke risico’s ontstaan in de praktijk, en hoe wordt aantoonbaar gestuurd op kwaliteit.

De AI Act (Verordening (EU) 2024/1689) brengt deze vragen onder een expliciet juridisch regime. De verordening definieert het begrip AI-systeem en rollen in de waardeketen en verbindt daaraan verplichtingen afhankelijk van het risicoprofiel van het systeem en de gebruikscontext.

De Business Information Services Library (BiSL®) is een framework voor Business informatiemanagement dat beschrijft hoe de vraagzijde van de informatievoorziening wordt georganiseerd: van dagelijks gebruik, via het realiseren van wijzigingen, tot sturing en strategische kaders.

De AI Act specificeert de juridische verplichtingen; BiSL® levert het procesmatige en organisatorische raamwerk waarmee die verplichtingen aantoonbaar kunnen worden ingebed in business informatiemanagement.

1.1 Doel, onderzoeksvraag en afbakening

Doel van dit whitepaper is het leveren van een compact en praktijkgericht referentiekader voor organisaties die AI-systemen willen inzetten of AI al inzetten. Centrale vraag:

> ***Hoe kunnen BiSL-processen worden ingezet om AI Act compliance aantoonbaar te maken, met specifieke aandacht voor gebruiksscenario's, risico's en impact?***

Afbakening: de focus ligt op organisatorische inbedding (BIM) en de compliance-producten[3] die nodig zijn om besluitvorming en beheersing te onderbouwen. Dit whitepaper vervangt geen juridisch advies en behandelt geen sectorspecifieke uitzonderingen in detail.

In dit whitepaper gaat het over de praktische consequenties van de AI Act. De strategische overwegingen van de organisatie als zodanig m.b.t. inzet en gebruik van AI vallen buiten de scope van dit whitepaper. Ook de wijze, waarop bij de inzet en gebruik van AI aansluiting gezocht zou moeten worden bij het enthousiasme, behoeften en wensen in de business organisatie, valt buiten de scope van dit whitepaper.

1.2 Doelgroep en gebruik van dit whitepaper

Dit whitepaper is primair geschreven voor zes rollen die binnen organisaties verantwoordelijkheid dragen voor de informatievoorziening en de governance daarvan.

De informatiemanager en functioneel beheerder (BIM) vinden in dit paper een handelingsperspectief: welke processen moeten worden ingericht of aangescherpt om AI-inzet aantoonbaar te beheersen. De compliance officer en privacy- of securityfunctionaris vinden de vertaling van AI Act-verplichtingen naar organisatorische beheersmaatregelen en contractuele kaders. De interne auditor en risicomanager vinden in de bijlagen A en B een auditbaar raamwerk.

[3] Een **compliance-product** is een document, bestand, record of bewijsstuk dat aantoont dat een organisatie voldoet aan specifieke wetten, voorschriften, normen of intern beleid. Het dient als tastbaar bewijs (evidence) tijdens audits of toezichthoudende controles dat processen correct zijn uitgevoerd en beheerst.

1.3 Relatie met andere AI-governance kaders

Dit whitepaper staat niet op zichzelf. Organisaties die al werken met bredere management- of risicoframeworks voor AI zullen herkenning vinden, maar ook vragen hebben over de verhouding tot die kaders. Onderstaande tabel laat zien hoe BiSL zich verhoudt tot respectievelijk ISO[4] 42001:2023, het NIST[5] AI Risk Management Framework en de EU AI Act.

Kader	Scope en focus	Wat BiSL toevoegt	Combinatie-advies
BiSL 4e editie	Vraagzijde informatievoorziening; procesmodel voor BIM	Centraal kader van dit whitepaper	Fundament; alle andere kaders worden hierin ingebed
ISO 42001:2023	Organisatiebreed AI-managementsysteem; PDCA-structuur	ISO beschrijft het wat op organisatieniveau; BiSL vult in hoe de vraagzijde dit operationaliseert	ISO 42001 als organisatiebreed dak; BiSL als uitvoeringsraamwerk
NIST AI RMF	Risicomanagement AI; vier kernfuncties: Govern, Map, Measure, Manage	NIST is risicogericht en technologieneutraal; BiSL vertaalt dit naar de IV-vraagzijde	NIST RMF voor risicotaxonomie; BiSL voor operationele inbedding
EU AI Act	Juridisch bindend regime voor AI in de EU	De AI Act stelt de norm; BiSL beschrijft de processen om daar invulling aan te geven	Compliance-baseline; BiSL, ISO 42001 en NIST RMF vullen gezamenlijk in hoe

Tabel 1 AI-governance kaders

1.4 Leeswijzer

Hoofdstuk 2 introduceert het conceptueel kader. Hoofdstuk 3 werkt de kernprocessen voor demand-use alignment uit. Hoofdstuk 4 behandelt datagovernance en lifecyclemanagement. Hoofdstuk 5 behandelt leveranciers- en contractmanagement. Hoofdstuk 6 presenteert een integrale roadmap. Hoofdstuk 7 sluit af met conclusies en aanbevelingen.

4 De Internationale Organisatie voor Standaardisatie (ISO) is een internationale organisatie die normen vaststelt. De organisatie is een samenwerkingsverband van nationale standaardisatieorganisaties in 163 landen.
5 NIST staat voor National Institute of Standards and Technology. Het is een niet-regelgevend agentschap van het Amerikaanse Ministerie van Handel dat standaarden, richtlijnen en technologieën ontwikkelt. Wereldwijd is NIST vooral bekend als dé autoriteit op het gebied van cybersecurity en databeveiliging

2. Conceptueel kader: BiSL en het risicogebaseerde AI Act-model

2.1 BiSL als vraagzijde-framework voor informatievoorziening

BiSL positioneert business informatiemanagement als de discipline die de business vertegenwoordigt richting IT-dienstverleners en die verantwoordelijk is voor de kwaliteit en continuïteit van de informatievoorziening. Het BiSL-procesmodel kent clusters voor dagelijks beheer (Gebruiksbeheer), het realiseren van veranderingen (Functionaliteitenbeheer en Verbindende processen op uitvoerend niveau), sturing (Sturende processen) en richtinggevend beleid (Richtinggevende processen).

Een belangrijk uitgangspunt is dat sturing niet alleen de dagelijkse activiteiten betreft, maar ook de incidentele activiteiten rond veranderingen en projecten. Daarmee biedt BiSL een geschikt kader om AI-toepassingen niet als “innovatieprojecten” te isoleren, maar als structurele componenten van de IV-portfolio te beheersen.

2.2 Risicobenadering

De AI Act definieert een “AI-systeem” als “een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen.”

Het inzetten en toepassen van dergelijke AI-systemen in bedrijfsprocessen brengt tal van risico's met zich mee. In de AI Act gaat het met name om de vraag hoe deze risico's beheerst kunnen worden. In de kern is de AI Act een risicogebaseerd model met 4 niveaus:

1. **Onaanvaardbaar risico**
   Deze toepassingen zijn verboden. Denk aan schadelijke manipulatie, uitbuiting van kwetsbaarheden, beoordeling van natuurlijke personen (social scoring), bepaalde vormen van op voorspellende wijze toezichthouden (predictive policing), ongerichte data extractie (scraping) van gezichtsbeelden[6], emotieherkenning op werk en in onderwijs, en bepaalde biometrische categorisering.
2. **Hoog risico**
   Deze systemen zijn toegestaan, maar alleen onder zware eisen. Dat geldt onder meer voor AI in bepaalde productveiligheidscontexten en voor gebruiksgevallen uit Bijlage III (AI Act), zoals biometrie, kritieke infrastructuur, onderwijs, werkgelegenheid, toegang tot essentiële publieke of private diensten, rechtshandhaving, migratie/asiel en rechtspleging. Voor zulke systemen gelden eisen rond risicobeheer, data governance, documentatie, menselijk toezicht, nauwkeurigheid, robuustheid en cyberbeveiliging. In specifieke situaties, namelijk bij hoog-risico-AI-systemen ingezet door publieke instellingen of private organisaties die publieke taken uitvoeren, geldt een beoordeling van de gevolgen voor de grondrechten door middel van een Fundamental Rights Impact Assessment (FRIA)[7] vóór ingebruikname.

[6] Het ongericht en geautomatiseerd verzamelen van gezichtsafbeeldingen uit online bronnen of camerabeelden, met als doel een database voor gezichtsherkenning op te bouwen of uit te breiden.
[7] Een effectbeoordeling op het gebied van de grondrechten, in het Engels “Fundamental Rights Impact Assessment” of afgekort “FRIA”) is een instrument voor organisaties om specifieke risico’s voor de rechten van (groepen) personen die waarschijnlijk zullen worden getroffen door gebruik van een hoog-risico AI-systeem in kaart te brengen en om te bepalen welke mitigerende maatregelen er nodig zijn in het geval die risico’s zich voordoen. FRIA geldt met name voor publieke instellingen of private organisaties met publieke taken. Ook gebruiksverantwoordelijken van bepaalde hoog-risico-AI-systemen voor kredietwaardigheid/kredietscore en levens-/ziekteverzekeringsrisico’s vallen onder de FRIA bepaling in artikel 27 van de AI Act.

3. **Beperkt risico**
   Hiervoor gelden vooral transparantieverplichtingen. Mensen moeten bijvoorbeeld weten dat zij met AI interageren of dat content kunstmatig is gegenereerd of gemanipuleerd.

4. **Minimaal of geen risico**
   Voor deze categorie legt de AI Act in de regel geen specifieke extra verplichtingen op voor het AI-systeem zelf. Ze blijven natuurlijk wel onder ander toepasselijk recht vallen, zoals de Algemene Verordening Gegevensbescherming (AVG), consumentenrecht of sectorspecifieke regels.

De nuance is wel belangrijk: de Europese Commissie communiceert dit als 4 niveaus, maar in de juridische systematiek van de verordening zie je vooral drie expliciete regelregimes voor AI-systemen terug: verboden praktijken, hoog-risico-AI, en AI met transparantieverplichtingen. Alles daarbuiten valt in de praktijk in de “minimaal/geen risico”-hoek. Dat volgt uit de risico gebaseerde aanpak in de AI Act zelf.

Naast de hoog-risico categorie kent de AI Act een aparte regeling voor General Purpose AI-systemen (**GPAI-systemen**), vastgelegd in artt. 51–56. GPAI-systemen zijn AI-modellen geschikt voor een breed scala aan taken, zoals grote taalmodellen (LLM’s), multimodale modellen en generatieve AI-systemen (bijv. Microsoft Copilot, ChatGPT, Google Gemini).

Voor de aanbieder van een GPAI-systeem gelden specifieke verplichtingen rond transparantie, technische documentatie en — bij modellen met systeemrisico — aanvullende eisen rond beveiliging en incidentmelding. Voor de **gebruiksverantwoordelijke** — de organisatie die een GPAI-systeem inzet — gelden die aanbiedersverplichtingen niet rechtstreeks, maar ontstaan wel degelijk organisatorische verplichtingen: passend gebruik, transparantie richting gebruikers (art. 50), en het voorkomen van verboden praktijken (art. 5).

Aandachtspunt voor BiSL is dat GPAI-modellen/AI-systemen gebaseerd op GPAI-modellen in de praktijk vaak worden ingezet via een tussenlaag: een aanbieder bouwt een product op basis van een onderliggend GPAI-model (bijv. een HR-systeem dat gebruikmaakt van een LLM voor het genereren van beoordelingsteksten). In dat geval moet bij Wijzigingenbeheer en Specificeren expliciet worden vastgesteld welke partij verantwoordelijk is voor welke complianceverplichting.

Aspect	Hoog-risico-AI (Bijlage III AI Act)	GPAI-systeem (artt. 51–56)
Typische use cases	Kredietscoring, CV-screening, uitkeringsbeoordelingen, biometrische identificatie	Samenvatten, concepten maken, Q&A, vertalen, codegeneratie, klantenserviceassistentie
Verplichtingen gebruiksverantwoordelijke (deployer)	Uitgebreid: passend gebruik, menselijk toezicht, logging[8], FRIA (publieke sector), incidentmelding	Beperkter: transparantie richting gebruikers, verboden praktijken vermijden, gebruiksbeleid
Primaire BiSL-processen	Wijzigingenbeheer, Specificeren, Toetsen en testen, Contractmanagement	Behoeftemanagement, Gebruikersondersteuning, Leveranciersmanagement
Risico op rolwijziging	Bij substantiële wijziging of doelwijziging	Bij het bouwen van een eigen applicatie op een GPAI-model

Tabel 2 Hoog risico versus GPAI-systemen

2.3 Rollen in de AI Act

De AI Act onderscheidt drie primaire rollen, elk met eigen verplichtingen.

Rol	Definitie	Typische situatie	Primaire verplichtingen
Aanbieder (provider)	Partij die een AI-systeem ontwikkelt of laat ontwikkelen en het op de markt brengt	Externe softwareleverancier die een hoog-risico AI-product aanbiedt	Technische documentatie, conformiteitsbeoordeling, CE-markering[9], registratie
Gebruiksverantwoordelijke (deployer)	Organisatie die een AI-systeem onder eigen verantwoordelijkheid inzet in een concrete context	Gemeente die een hoog-risico AI-systeem inzet bij uitkeringsbeoordelingen	Passend gebruik, menselijk toezicht, logging bewaren, betrokkenen informeren
Distributeur / importeur	Tussenpartij in de keten; kan aanbieder worden bij substantiële wijziging	Organisatie die een AI-component doorlevert aan eindgebruikers	Transparantie over onderleveranciers; bij substantiële wijziging: aanbiedersverplichtingen

Tabel 3 Rollen en verplichtingen

[8] de geautomatiseerde, chronologische registratie van gebeurtenissen en handelingen binnen een systeem. Het fungeert als een digitaal logboek waarin software, servers of netwerken nauwkeurig bijhouden wat er gebeurt en wanneer, zoals systeemfouten, succesvolle inlogpogingen of het wijzigen van bestanden.

[9] Een CE-markering (Conformité Européenne) is een verplicht label op producten waarmee de fabrikant verklaart dat deze voldoen aan de strenge Europese eisen voor veiligheid, gezondheid en milieu. Zonder CE-markering mag een product niet worden verkocht binnen de Europese Economische Ruimte

Aandachtspunt voor BiSL®: De rolbepaling is geen eenmalige vaststelling maar een onderdeel van het proces wijzigingenbeheer. Zodra een organisatie het doel of de configuratie van een AI-systeem substantieel wijzigt, moet opnieuw worden beoordeeld of de rol verschuift van gebruiksverantwoordelijke naar aanbieder.

2.4 Implicatie voor organisaties: compliance als “evidence supply chain”

AI Act-compliance is in de praktijk niet één document of één toets, maar een keten van bewijsvoering (evidence) over gebruiksscenario, doel, risico’s, beheersmaatregelen, besluitvorming en monitoring. BiSL-processen produceren van nature dergelijke evidence, mits AI expliciet als beheerobject wordt opgenomen in de scope van BIM.

2.5 Tussenconclusie

Hoofdstuk 2 maakt duidelijk dat AI Act-compliance pas werkbaar wordt wanneer de juridische risicobenadering wordt vertaald naar herkenbare besturings- en beheerprocessen. De AI Act bepaalt welke risicocategorieën, rollen en verplichtingen gelden; BiSL biedt het vraagzijde-raamwerk om deze organisatorisch te operationaliseren binnen de informatievoorziening.
AI-systemen moeten daarom niet als losse technologische toepassingen worden behandeld, maar als structurele IV-componenten met een expliciet doel, gebruikscontext, eigenaar, risicoprofiel en bewijsvoering. Daarbij vraagt vooral de rolbepaling blijvende aandacht, omdat wijzigingen in doel, configuratie of gebruik kunnen leiden tot andere verplichtingen.
Daarmee introduceert hoofdstuk 2 het centrale uitgangspunt voor de rest van het whitepaper: AI-compliance is een evidence supply chain. Hoofdstuk 3 werkt uit hoe deze keten start met beleid, kaders, sturing en traceerbare besluitvorming.

3. Beleid, kaders en sturing

3.1 AI-beleid als onderdeel van informatiebeleid

AI-beleid is geen losstaand technologiebeleid, maar een verbijzondering van het informatiebeleid en, waar relevant, van het bredere bedrijfsbeleid. Zodra AI-systemen worden ingezet in primaire of ondersteunende processen, worden zij onderdeel van de informatievoorziening en daarmee ook van de reguliere bestuurlijke vraagstukken rond eigenaarschap, kwaliteit, risico, continuïteit en verantwoording. Vanuit BiSL ligt het daarom voor de hand om AI-beleid te verankeren in de richtinggevende en sturende processen van business informatiemanagement.

De AI Act vraagt niet alleen om technische maatregelen, maar ook om aantoonbare organisatorische keuzes: welk gebruik is toegestaan, welk doel wordt ondersteund, welke risico's zijn onderkend, welke beheersmaatregelen gelden, wie toezicht houdt en welke documentatie beschikbaar moet zijn. AI-compliance vraagt daarom om samenhang tussen beleid, portfolio, governance, sourcing en uitvoering. In dit whitepaper wordt die samenhang benaderd als een evidence supply chain: een keten van beleidskaders, besluiten, registraties, controles en rapportages.

Onderstaande tabel laat zien hoe de BiSL-richtinggevende processen bijdragen aan organisatiebreed AI-beleid en welke beleidsartefacten daaruit voortkomen.

BiSL-proces	Beleidsbijdrage aan AI-beleid	Concrete producten
Bepalen bedrijfsprocesont-wikkelingen	Maakt zichtbaar waar AI relevant wordt in primaire en ondersteunende processen, en waar risico's ontstaan voor kwaliteit, dienstverlening, rechtsgelijkheid of controleerbaarheid.	Analyse bedrijfsprocesontwikkelingen met AI-impact; domeinkaart AI-toepassingen; overzicht van kritische beslispunten; afbakening van toegestane en niet-toegestane AI-toepassingen; impact en eisen voor informatiekwaliteit
Bepalen technologieont-wikkelingen	Brengt relevante AI-technologieën, marktontwikkelingen en technologische risico's in beeld.	Technologieverkenning AI; standpuntnota (position paper) over generatieve AI en voorspellende modellen; beleidsnotitie met uitgangspunten voor uitlegbaarheid, transparantie, logging en beheersbaarheid.
Bepalen keten-ontwikkelingen	Brengt relevante eisen, kansen en risico's van AI-gebruik in de keten in beeld	Hoe beïnvloedt AI-gebruik de informatie, informatisering en processen in de keten?
Informatie-lifecyclemanagement	Legt beleid vast voor de levenscyclus van datasets, modellen, prompts, logging, uitkomsten en documentatie.	Lifecyclebeleid voor AI-objecten; classificatiekader voor data en modellen; beleid voor versiebeheer, bewaartermijnen, herbeoordeling en buitengebruikstelling.
Informatie-portfoliomanage-ment	Bepaalt welke AI-initiatieven strategisch relevant zijn en onder welke voorwaarden zij prioriteit krijgen.	AI-portfolio; prioriteringskader; businesscriteria voor waarde en risico; bestuurlijke besluitnota's.

BiSL-proces	Beleidsbijdrage aan AI-beleid	Concrete producten
Strategie inrichting IV-functie	Richt governance, rollen, verantwoordelijkheden en escalatie in voor verantwoord AI-gebruik.	Governance-model voor AI; RACI-matrix; mandaatregeling; escalatiepad; rolbeschrijvingen.
Relatiemanagement gebruikersorganisatie	Legt kaders vast voor de verankering van het AI-beleid in de organisatie	Vastgelegde verantwoordelijkheden en benodigde competenties voor verantwoord gebruik van AI.
Leveranciersmanagement	Geeft richting aan sourcingkeuzes en eisen aan externe AI-diensten en leveranciers.	Sourcingbeleid voor AI; standaard contracteisen; leveranciersbeoordelingskader; due diligence-checklist; afspraken over logging, incidentmelding, modelwijzigingen, auditrechten en exitstrategie.
Ketenpartnersmanagement	Borgt dat AI-beleid ook geldt in ketens en gegevensuitwisseling met partners.	Ketenafspraken AI; gegevensuitwisselingsprotocol; verantwoordelijkhedenmatrix; escalatie- en meldstructuur; ketenimpactanalyse.
Informatiecoördinatie	Zorgt voor samenhang en afstemming tussen beleid en plannen voor de IV, in overeenstemming met de organisatorische kaders.	Integraal AI-beleidskader; besluitvormingskalender; samenhang notitie; overzicht van normen en kaders; bestuurlijke afstemmingsagenda.

Tabel 4. Bijdrage van BiSL-richtinggevende processen aan AI-beleid

3.2 Behoeftemanagement: prioritering, kwaliteitssturing en compliancekaders

Behoeftemanagement is de plaats waar AI-beleid wordt vertaald naar concrete kaders. Het proces kanaliseert nieuwe behoeften vanuit de business en toetst of die behoefte past binnen het geldende beleids-, risico- en compliancekader.

Voor AI vervult Behoeftemanagement twee functies. Enerzijds kanaliseert het nieuwe behoeften vanuit de business: waar is AI-ondersteuning gewenst, welk probleem moet worden opgelost en welke waarde wordt beoogd. Anderzijds toetst het of die behoefte past binnen het geldende beleids-, risico- en compliancekader.

In AI-context leidt dit tot vier typen kaders: toepassingskaders (waar is AI passend), kwaliteitskaders (datakwaliteit, uitlegbaarheid, logging), portfoliokaders (prioritering op waarde, risico en compliance-last) en competentiekaders (kennis en bevoegdheden voor verantwoord AI-gebruik).

Daarmee borgt Behoeftemanagement dat AI-inzet niet opportunistisch plaatsvindt, maar binnen expliciete kaders en met structurele kwaliteitssturing. Organisatorische randvoorwaarden worden zo al in de vraag- en prioriteringsfase meegenomen.

AI-geletterdheid als randvoorwaarde voor verantwoord gebruik
Een belangrijke randvoorwaarde voor verantwoord AI-gebruik is AI-geletterdheid[10]. De AI Act verlangt dat organisaties die AI-systemen ontwikkelen of gebruiken passende maatregelen treffen om medewerkers en andere betrokkenen voldoende kennis en begrip te geven van AI-systemen, hun mogelijkheden, beperkingen, risico's en de context waarin zij worden toegepast. Tevens dienen medewerkers en andere betrokkenen ervan doordrongen te worden dat ze niet op eigen initiatief en inzicht gebruik kunnen en mogen maken van AI-systemen.

AI-geletterdheid is daarmee geen vrijblijvende opleidingsactiviteit, maar een organisatorische beheersmaatregel die direct bijdraagt aan passend gebruik, menselijk toezicht, risicosignalering en naleving van transparantieverplichtingen.

Binnen BiSL ligt de beleidsmatige verankering van AI-geletterdheid primair bij **Behoeftemanagement**. Dit proces vertaalt AI-beleid en compliance-eisen naar competentiekaders: welke kennis, vaardigheden en bevoegdheden zijn nodig voor gebruikers, functioneel beheerders, proceseigenaren en informatiemanagers om AI verantwoord te kunnen inzetten en beoordelen. Daarbij gaat het niet alleen om algemene kennis over AI, maar vooral om contextgebonden kennis: het doel van het AI-systeem, de betekenis en beperkingen van output, de risico's van automation bias[11], de escalatiecriteria en de situaties waarin menselijk ingrijpen noodzakelijk is.

Relatiemanagement gebruikersorganisatie borgt vervolgens dat deze kaders daadwerkelijk landen in de gebruikersorganisatie. Dit proces zorgt voor afstemming met management, proceseigenaren, HR, opleidingsfuncties en gebruikersvertegenwoordigers over rollen, verantwoordelijkheden en gedragsverwachtingen rond AI-gebruik. Daarmee wordt AI-geletterdheid onderdeel van de reguliere sturing op de inrichting en professionalisering van de IV-functie, in plaats van een eenmalige training bij introductie van een systeem.

Het AI-register als fundament van BIM-scope

Het AI-register is de meest concrete eerste stap naar aantoonbare AI-governance. Het register fungeert als centraal overzicht van alle AI-toepassingen en vormt de basis waarop Wijzigingenbeheer, Behoeftemanagement en Contractmanagement kunnen sturen.

[10] AI-geletterdheid is vanaf 2 februari 2025 van toepassing
[11] **Automation bias** (automatiseringsbias) is de menselijke neiging om blindelings te vertrouwen op de adviezen, resultaten of beslissingen van geautomatiseerde systemen.

Sectie	Veld	Vereist	BiSL-proces
A — Identificatie	Naam toepassing, versie, leverancier	Verplicht	Behoeftemanagement
A — Identificatie	Beoogd doel en procesinbedding	Verplicht	Specificeren
A — Identificatie	AI Act risicoklasse (via Quickscan)	Verplicht	Wijzigingenbeheer
A — Identificatie	Rol organisatie (aanbieder of gebruiksverantwoordelijke)	Verplicht	Wijzigingenbeheer
B — Eigenaarschap	Systeemeigenaar (naam en functie)	Verplicht	Strategie inrichting IV-functie
B — Eigenaarschap	Business informatiemanager	Verplicht	Strategie inrichting IV-functie
C — Compliance	Use case-dossier aanwezig (locatie)	Verplicht	Toetsen en testen
C — Compliance	DPIA/FRIA uitgevoerd (datum, locatie)	Hoog-risico: verplicht	Toetsen en testen
C — Compliance	Logging ingericht (bewaartermijn)	Verplicht	Operationele IT-aansturing
C — Compliance	Datum volgende herbeoordeling	Verplicht	Planning & control

Tabel 5 Het AI-register

3.3 Planning & control: van beleidskader naar uitvoerbare AI-besturing

Waar Behoeftemanagement bepaalt wat de organisatie met AI wil bereiken en onder welke voorwaarden, zorgt Planning & Control voor uitvoerbaarheid. Dit proces vertaalt beleidskeuzes naar capaciteit, planning, samenhang en bestuurlijke ritmiek.

Voor AI betekent dit dat niet alleen de inhoud van een initiatief wordt beoordeeld, maar ook de haalbaarheid ervan in termen van verandercapaciteit, toetsmomenten, leveranciersafstemming, training, incidentprocedures en periodieke evaluatie. Zonder die planning blijven beleidskaders bestuurlijke intenties.

In AI-context richt Planning & control zich op vijf onderwerpen: capaciteitsplanning, tijdsplanning en veranderkalender, periodieke reviews, beheer van afhankelijkheden en escalatie- en bijsturingsmomenten. Concreet leidt dit tot producten als een AI-jaarplan, kwartaalroadmap, capaciteitsplan, reviewkalender, managementdashboard en periodieke stuurrapportage.

De meerwaarde van Planning & control ligt in de operationalisering van beleid. Het proces zorgt dat de juiste capaciteit met de juiste competenties beschikbaar is en borgt dat monitoring, toezicht en herbeoordeling onderdeel worden van de reguliere besturingscyclus.

3.4 Aankopen en (door)ontwikkelen van AI-systemen

De beleids- en sturingslaag krijgt pas betekenis wanneer zij doorwerkt in de veranderketen. Binnen BiSL vormen de processen Wijzigingenbeheer, Specificeren, Vormgeven niet-geautomatiseerde informatievoorziening, Toetsen en testen, Voorbereiden transitie en Transitie samen de route van behoefte naar ingebruikname. In AI-context is deze keten van belang omdat juist hier het gebruiksdoel wordt gespecificeerd, risico-inschatting wordt geconcretiseerd en acceptatievoorwaarden worden geborgd.

3.4.1 Wijzigingenbeheer

Wijzigingenbeheer is het formele besluitvormingspunt waarop AI-ideeën worden omgezet in gecontroleerde wijzigingen. De kern is traceerbare besluitvorming: waarom wordt een AI-toepassing wel of niet ingevoerd, met welke beheersmaatregelen en onder welke voorwaarden? In de praktijk vraagt dit om een quickscan of impactanalyse per AI-initiatief met ten minste een scope-check, een toets op verboden of hoog-risico-toepassingen, en een eerste rolbepaling in de waardeketen en een inventarisatie van aanvullende eisen aan logging, toezicht, impactbeoordelingen en monitoring. De uitkomst hoort expliciet onderdeel te zijn van het wijzigingsbesluit.

Voor alle systemen geldt, op basis van de AVG, de verplichting tot een 'data protection impact assessment' (DPIA) 12 wanneer er sprake is van een verhoogd privacyrisico.

In het geval dat er sprake is van de inzet van een hoog-risico-AI-systeem met specifieke risico's voor de rechten van (groepen) personen die waarschijnlijk zullen worden getroffen door het gebruik daarvan, dient volgens de AI Act een "Fundamental Rights Impact Assessment" ("**FRIA**") te worden uitgevoerd om te bepalen welke mitigerende maatregelen er nodig zijn in het geval die risico's zich voordoen en welke mitigerende maatregelen getroffen kunnen worden. Organisaties die al een DPIA-proces hebben ingericht vanuit de AVG, beschikken over een bruikbaar fundament voor de FRIA. Beide instrumenten vragen om een gestructureerde impactbeoordeling vóór ingebruikname.

> **Praktische aanbeveling voor business informatiemanagement:** behandel de FRIA niet als een nieuw en los instrument, maar als een uitbreiding van het bestaande DPIA-proces. Voeg in het use case-dossier (§3.4.2) een aparte sectie "grondrechtenbeoordeling" toe die bij hoog-risico toepassingen verplicht wordt ingevuld. Koppel de uitvoering aan Toetsen en testen, zodat de FRIA een formele go/no-go voorwaarde wordt.

Voorbeeld 1 — Hoog-risico AI: Geautomatiseerde kredietscoring voor MKB-leningen (financiële instelling). Risicoklasse: hoog-risico, Bijlage III punt 5(b) (AI Act). Het AI-model genereert een kredietscore als input; de beslissing blijft bij een menselijke medewerker. Vereist: FRIA, conformiteitsbeoordeling, EU-databaseregistratie. Logging: input, score en kredietbesluit bewaard minimaal 5 jaar.

Voorbeeld 2 — General-purpose AI (GPAI) model: AI-assistent voor het samenvatten van beleidsdocumenten (gemeente). GPAI, art. 50. Medewerkers gebruiken Copilot voor het samenvatten van raadsstukken; output wordt altijd door een medewerker beoordeeld. Geen FRIA vereist. Werkinstructie en meldprocedure verplicht vóór livegang.

[12] Zie de website van de autoriteit persoonsgegevens voor meer informatie over dit onderwerp. https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia

Aspect	DPIA (AVG / art. 35)	FRIA (AI Act / art. 27)	BiSL-proces
Wanneer verplicht	Bij verwerkingen met hoog privacyrisico	Bij hoog-risico AI ingezet door publieke instellingen of private organisaties met publieke taken. Tevens hoog-risico-AI-systemen voor kredietwaardigheid /kredietscore en levens-/ziekteverzekeringsrisico's	Wijzigingenbeheer — als go/no-go criterium in Quickscan
Focus	Bescherming persoonsgegevens en privacyrechten	Grondrechten breder: gelijkheid, non-discriminatie, toegang tot rechter	Specificeren — aparte sectie in use case-dossier
Timing	Vóór aanvang verwerking	Vóór ingebruikname hoog-risico systeem	Voorbereiden transitie — FRIA als go/no-go voorwaarde
Aanbeveling	Beide bevatten overlappende elementen; een gecombineerd DPIA/FRIA-document is mogelijk	De FRIA vereist aanvullend: beoordeling op groepsniveau en raadpleging vertegenwoordigers	Behoeftemanagement — DPIA-FRIA-combinatie als kwaliteitsnorm voor hoog-risico AI

Tabel 6 DPIA en FRIA: samenhang en verschillen

3.4.2 Specificeren: het AI-use case-dossier

Specificeren is het proces waarin doelen, randvoorwaarden en functionele behoeften worden uitgewerkt tot eenduidige specificaties. Voor AI is dat cruciaal, omdat juist hier het doel, de gebruikscontext en de acceptatiecriteria expliciet moeten worden gemaakt.

Een **AI-use case-dossier** vormt het kernproduct en bevat ten minste: het doel en de procesinbedding, de betrokken gebruikersrollen, de verdeling tussen systeem handelen en menselijk besluit, input- en outputdefinities, datakwaliteitseisen, acceptatiecriteria, testaanpak en eisen voor logging, monitoring en escalatie. Daarmee ontstaat één samenhangende basis voor realisatie, toetsing en verantwoording. In **bijlage D** zijn twee contrasterende use-case voorbeelden uitgewerkt.

3.4.3 Vormgeven niet-geautomatiseerde informatievoorziening

AI-compliance wordt niet alleen bepaald door het systeem, maar ook door de manier waarop mensen ermee werken. Dit proces richt zich daarom op werkinstructies, procedures, handleidingen en procesafspraken die menselijke interventie, interpretatie en communicatie borgen.

Voor AI betekent dit dat expliciet moet worden vastgelegd hoe gebruikers AI-uitkomsten interpreteren, wanneer zij moeten afwijken van een systeemadvies, hoe twijfel of incidenten worden gemeld en hoe transparantie richting betrokkenen wordt georganiseerd. Hier worden menselijke verantwoordelijkheid en operationele werkwijze concreet gemaakt.

3.4.4 Toetsen en testen

In het proces Toetsen en testen wordt beoordeeld of aan alle verplichtingen is voldaan. Naast het testen van de functionaliteit moet worden vastgesteld of de AI-toepassing in de praktijk voldoet aan het doel, de acceptatiecriteria, de eisen voor logging en monitoring en de randvoorwaarden voor menselijk toezicht.

Voor een goede acceptatietest moet de testset naast de functionele tests, ook use-case tests, scenarioanalyses, negatieve tests, logging-controles en validatie van de niet-geautomatiseerde werkwijze omvatten.

Het resultaat is niet alleen een testverslag, maar ook een expliciet advies over verantwoorde ingebruikname, restrisico's en voorwaarden voor livegang.

3.4.5 Voorbereiden transitie

Voorbereiden transitie richt zich op probleemloze ingebruikname. Voor AI betekent dit dat vóór ingebruikname aantoonbaar moet zijn dat gebruikers en beheerders beschikken over werkinstructies, trainingsmateriaal, escalatieprocedures en communicatie over het gebruik van AI. Voor hoog-risico of maatschappelijk gevoelige toepassingen hoort daarbij ook oefening met praktijkscenario's, zoals afwijkende output, vermoedelijke bias, incidentmelding en het toepassen van menselijk toezicht. Het trainingsregister, de beschikbaarheid van instructies en de afgeronde readiness check vormen daarbij auditbaar bewijs dat AI-gebruik niet alleen technisch, maar ook organisatorisch verantwoord is voorbereid.

Producten zijn onder meer een implementatieplan, trainingsplan, autorisatiematrix, communicatieplan, supportinstructies, ketenafspraken en een overzicht van openstaande restrisico's. Niet alleen het systeem moet klaar zijn, maar ook de organisatie.

3.4.6 Transitie

In Transitie worden de resultaten van de wijzigingsketen daadwerkelijk in gebruik genomen. Voor AI vraagt dit om een gecontroleerde ingebruikname, inclusief actieve monitoring, beschikbare logging, operationele meldroutes, gebruikerscommunicatie en waar nodig een tijdelijke observatieperiode.

Een AI-transitie is pas afgerond wanneer de toepassing niet alleen technisch live is, maar ook beheerst is overgedragen naar beheer en gebruik.

3.5 Beheer en gebruik van AI-systemen

Na ingebruikname verschuift de aandacht van verandering naar dagelijks gebruik en beheer. Binnen BiSL ligt het zwaartepunt dan bij Gebruikersondersteuning, Operationele ketenafstemming en Operationele IT-aansturing. In deze processen ontstaat veel van de dagelijkse evidence die nodig is om AI-gebruik blijvend te beheersen.

3.5.1 Gebruikersondersteuning

Gebruikersondersteuning is de plek waar dagelijks gebruik zichtbaar wordt. Het proces moet onderscheid kunnen maken tussen gebruiksvragen, functionele fouten, datakwaliteitsproblemen, onbegrijpelijke of ongewenste uitkomsten, klachten van betrokkenen en signalen van systemische risico's.

Dat vraagt om passende meldclassificatie, kennis van de AI-toepassing en duidelijke escalatieroutes naar Wijzigingenbeheer, Behoeftemanagement, leveranciers of compliancefuncties, zoals interne controle. Daarmee levert Gebruikersondersteuning first-line evidence op in de vorm van meldingenregisters, signaleringsrapportages, issuepatronen en terugkoppelingen naar de sturende processen.

3.5.2 Operationele ketenafstemming

Wanneer AI-systemen data of uitkomsten delen met ketenpartners, wordt Operationele ketenafstemming essentieel. Hier worden afspraken over gegevensuitwisseling, kwaliteitsproblemen, veiligheidsmaatregelen en incidentcommunicatie bewaakt in de dagelijkse praktijk.

Het proces moet niet alleen reageren op verstoringen, maar ook signaleren wanneer bestaande ketenafspraken niet langer toereikend zijn door veranderend gebruik, nieuwe risico's of gewijzigde gegevensstromen. Daarmee wordt geborgd dat AI-gebruik ook buiten de eigen organisatiegrens beheerst blijft.

3.5.3 Operationele IT-aansturing

Operationele IT-aansturing zorgt ervoor dat de dagelijkse dienstverlening van IT-partijen blijft aansluiten op de eisen van business en BIM. Voor AI gaat het daarbij om logging, monitoring, performance, beveiliging, releasestabiliteit en incidentrespons.

Omdat veel AI-toepassingen afhankelijk zijn van externe modellen, cloud-omgevingen, API's of SaaS-componenten, moet dit proces niet alleen sturen op beschikbaarheid, maar ook op logvolledigheid, patchstatus, retentie-instellingen, monitoringdashboards en de impact van leverancierswijzigingen op gebruik en compliance. Daarmee vormt Operationele IT-aansturing de operationele sluitsteen van de compliance-keten.

3.5.4 De AI-monitoringfunctie als sluitstuk van dagelijks beheer

Post-deployment monitoring is in de AI Act geen optionele maatregel maar een expliciete verplichting voor gebruiksverantwoordelijken van hoog-risico AI-systemen[13]. Voor business informatiemanagement betekent dit dat monitoring niet als technische taak mag worden weggezet bij de IT-dienstverlener, maar als een gedeelde verantwoordelijkheid van de eerste en tweede lijn moet worden ingericht.

Een effectieve AI-monitoringfunctie bestaat uit vier samenhangende elementen die elk in een specifiek BiSL-proces zijn verankerd:

1. ***Wat*** *wordt gemonitord* wordt bepaald in Behoeftemanagement en Specificeren: prestatiedrift van het model, datakwaliteitsafwijkingen, onverwachte of ongewenste uitkomsten, en overrides door gebruikers (gevallen waarin een menselijke medewerker afwijkt van het systeemadvies). Deze monitoringobjecten worden vastgelegd in het monitoringplan (Bijlage B, artefact 11).
2. ***Hoe*** *wordt gemonitord* is de technische invulling die Operationele IT-aansturing borgt: logging van input/output/overrides, dashboards voor drift-detectie, retentie-instellingen en toegangsautorisaties voor de logomgeving.
3. ***Wie*** *monitort* is een rolkwestie die in de governance-inrichting (Strategie inrichting IV-functie, RACI) wordt vastgelegd. In de praktijk zijn drie rollen betrokken: de functioneel beheerder bewaakt dagelijks de dashboards en meldt afwijkingen; de informatiemanager beoordeelt maandelijks de signaleringsrapportages; de compliance officer of risicomanager toetst kwartaalrapportages op compliance-implicaties.
4. ***Wanneer*** *leidt monitoring tot actie* is de escalatielogica die Gebruikersondersteuning en Wijzigingenbeheer met elkaar verbindt.

[13] "Voor gebruiksverantwoordelijken volgt monitoring primair uit art. 26; art. 72–73 zijn relevant in de ketenafstemming met providers."

Drie escalatieniveaus zijn te onderscheiden:

Escalatieniveau	Signaal	Actie	BiSL-proces
1 — Operationeel	Afwijkingen binnen drempelwaarden	Afhandeling via Gebruikersondersteuning; registratie meldregister	Gebruikersondersteuning
2 — Structureel	Drift of patroon van overrides buiten drempelwaarden	Activering Wijzigingenbeheer; herbeoordeling model, data of gebruikscontext	Wijzigingenbeheer en Behoeftemanagement
3 — Ernstig incident	Systematische fout, grondrechten-schending, meldplichtig incident	Incidentprocedure + meldplicht toezichthouder; Contractmanagement informeert leverancier (art. 73)	Contractmanagement, Operationele IT-aansturing

Tabel 7 Escalatieniveaus

3.6 Tussenconclusie

Verantwoord AI-gebruik begint niet bij de technologie zelf, maar bij heldere beleidskeuzes, expliciete kaders en bestuurbare processen. Hoofdstuk 3 laat zien hoe AI-beleid binnen BiSL wordt vertaald naar concrete besluitvorming over behoefte, prioriteit, risico, gebruikscontext en kwaliteitscriteria. Behoeftemanagement, Planning & control, Wijzigingenbeheer en Specificeren vormen daarbij de kern van de vraagzijde: zij bepalen waarom AI wordt ingezet, onder welke voorwaarden dat verantwoord is en welke evidence nodig is om dit aantoonbaar te maken.
Daarmee ontstaat een gecontroleerde keten van idee tot ingebruikname en beheer. Use case-dossiers, AI Act Quickscans, acceptatiecriteria, testresultaten, transitieplannen, gebruikersinstructies en meldingen uit dagelijks gebruik maken AI-compliance traceerbaar en herhaalbaar. De volgende hoofdstukken verdiepen twee randvoorwaarden voor deze beheersing: hoofdstuk 4 werkt datagovernance en lifecyclemanagement uit; hoofdstuk 5 behandelt de beheersing van leveranciers en contractuele afspraken in de AI-waardeketen.

4. Data governance en lifecyclemanagement

4.1 Data als asset binnen BiSL

Governance van data is geen “IT-detail”, maar een verantwoordelijkheid van de business. AI-toepassingen gebruiken vaak combinaties van stamgegevens (masterdata), transactiegegevens en referentiegegevens, en genereren nieuwe afgeleide data (scores, aanbevelingen, content). Dit vergt expliciete afspraken over herkomst, kwaliteit, bewaartermijnen en uitwisseling met ketenpartners. Dit hoofdstuk verbindt de eisen uit de AI Act rond data en monitoring met de BiSL-processen Beheer bedrijfsinformatie (operationele kwaliteit van data), Behoeftemanagement (kaders) en de richtinggevende processen rond informatie-lifecycle die samen het raamwerk vormen om structureel te borgen dat aan de eisen wordt voldaan.

4.2 AI Act: datavereisten, monitoring en logging als compliance-object

De AI Act stelt eisen aan de datasets die worden gebruikt voor de training van hoog-risico AI-systemen:

Voor hoog-risico AI-systemen die worden getraind met data stelt de AI Act eisen aan datasets voor training, validatie en tests, inclusief praktijken voor databeheer (oorsprong, verzameling, opschoning, bias-beoordeling, aannames). Daarnaast wordt van gebruiksverantwoordelijken verwacht dat zij de werking monitoren, zo nodig aanbieders informeren en logs bewaren gedurende een passende periode (ten minste zes maanden wanneer logs onder hun controle vallen).

Beheer bedrijfsinformatie operationaliseert datagovernance door datakwaliteitsnormen te definiëren, periodiek te meten en afwijkingen via issuebeheer en rapportage te sluiten met aantoonbaar bewijsmateriaal (dashboards, issue registers, control evidence).

Behoeftemanagement vertaalt compliance- en businessdoelen naar toetsbare kaders (requirements catalogue, KPI-set, acceptatiecriteria) en prioriteert de benodigde governance-maatregelen.

De richtinggevende processen rond de informatie-lifecycle verankeren dit in organisatiebrede standaarden en lifecycle-beleid (classificatie, retention, metadata/lineage en auditstrategie), zodat governance en monitoring herhaalbaar en consistent blijven over tijd, domeinen en ketens.

4.3 Praktische inrichting: het AI Data & Monitoring Control Set

Organisaties kunnen datagovernance operationaliseren met een beperkte set standaardcontroles die per AI-use-case worden ingevuld. Onderstaande set is bedoeld als minimum voor auditbaarheid:

#	Artefact	Owner (BiSL)	Doel / inhoud	Cadans	Hoog-risico
1	Dataherkomst-register	BBI	Herkomst, doel, grondslag, datakwaliteit-indicatoren	Kwartaal + bij wijziging	V
2	Bias & representativiteit-analyse	BBI	Welke groepen kunnen worden benadeeld; mitigaties	Per initiatief + jaarlijks	V

#	Artefact	Owner (BiSL)	Doel / inhoud	Cadans	Hoog-risico
3	Datakwaliteit-scorecard	BBI	KPI's, trends, drempels, uitzonderingen	Wekelijks/maandelijks	A
4	Data Issueregister	BBI	Issues, impact, eigenaar, acties, status	Continu	V
5	Logging-ontwerp	BM	Logscope, bewaartermijnen, toegang, integriteit	Jaarlijks + bij wijziging	V
6	Monitoringdashboard	BM	Driftdetectie, performance, incidenten, escalaties	Kwartaalreview	V
7	Dataset datasheet	BBI	Herkomst, populatie, representativiteit, beperkingen	Per dataset + bij wijziging	V
8	Compliance evidence pack	BBI	Bewijsbundel: dashboards, logsamples, reviews, CAPA	Kwartaal/halfjaar	A

Tabel 8 Minimum set aan standaardcontroles ten behoeve van auditbaarheid

Legenda: V = Verplicht (noodzakelijk als compliance evidence bij hoog-risico AI); A = Sterk aanbevolen. BBI = Beheer Bedrijfsinformatie; ILM = Informatie-Lifecyclemanagement; BM = Behoeftemanagement.

Deze standaardcontroles zijn overigens grotendeels een verbijzondering voor AI van het bedrijfsinformatiemodel, zoals dat in BiSL is beschreven.

4.4 Lifecyclemanagement: continual compliance

AI-systemen veranderen door nieuwe data, modelupdates en aanpassingen in gebruik. Daarom is "continual compliance" essentieel: bij elke significante wijziging in beoogd doel, inputdata of autonomie moet opnieuw worden beoordeeld welke risico's ontstaan en/of bestaande maatregelen volstaan.

BiSL biedt hiervoor een natuurlijk mechanisme: wijzigingsverzoeken worden via Wijzigingenbeheer beoordeeld, gespecificeerd en in releases doorgevoerd, waarna acceptatie en transitie plaatsvinden. Voor AI betekent dit dat herbeoordeling en herclassificatie expliciete stappen worden in het wijzigingsproces.

4.5 Tussenconclusie

Verantwoord AI-gebruik is alleen aantoonbaar wanneer data, logging en monitoring expliciet als beheerobjecten binnen business informatiemanagement worden ingericht. Hoofdstuk 4 laat zien dat datagovernance geen technisch randonderwerp is, maar een structurele businessverantwoordelijkheid: herkomst, kwaliteit, representativiteit, bias, bewaartermijnen, logging en monitoring bepalen in belangrijke mate of AI-systemen betrouwbaar, uitlegbaar en auditbaar kunnen functioneren. Beheer bedrijfsinformatie, Behoeftemanagement en Informatie-lifecyclemanagement vormen samen het BiSL-raamwerk waarmee deze eisen worden vertaald naar concrete controles, registraties, dashboards en periodieke herbeoordeling. Daarmee verschuift compliance van een eenmalige toets vóór ingebruikname naar continual compliance gedurende de volledige levenscyclus van data, model, gebruikscontext en besluitvorming. Hoofdstuk 5 werkt vervolgens uit hoe deze beheersing ook contractueel en organisatorisch in de leveranciersketen moet worden geborgd.

5. Leveranciers- en contractmanagement

Veel AI-functionaliteit wordt extern afgenomen (SaaS, cloud-AI, generieke modellen, API's). De organisatie die het systeem inzet blijft echter verantwoordelijk voor passend gebruik en governance en alle compliance evidence waaruit dat moet blijken. Dit hoofdstuk beschrijft hoe BiSL-processen Contractmanagement en Leveranciersmanagement worden gebruikt om de AI-waardeketen contractueel en operationeel te beheersen.

5.1 Contractmanagement: opdrachtgeversrol en SLA-bewaking

Contractmanagement is verantwoordelijk voor het maken van adequate afspraken over de geautomatiseerde IV en de dienstverlening door IT-dienstverleners, en voor het bewaken en verbeteren daarvan. Voor AI-componenten betekent dit dat contracten niet alleen beschikbaarheid en performance bevatten, maar ook compliance-leveringen: documentatie, transparantie, logging-mogelijkheden, incidentmeldingen en ondersteuning bij audits.

Clausule	Inhoud	Relevantie AI Act
Beoogd doel en gebruiksbeperkingen	Expliciete intended purpose (beoogd doel) en verboden gebruik; wijzigingsprocedure bij doelwijziging	Art. 9, 13: risicobeheer en transparantie
Documentatielevering	Technische documentatie en gebruiksinstructies; updates bij releases	Art. 13, 14: transparantie en menselijk toezicht
Logging & audit	Exporteerbare logs, log-schema, bewaartermijnen, toegang voor audits	Art. 12, 72: logging en monitoring
Incidentmelding & samenwerking	Reactietijd (Time to notify), escalatiepad, ondersteuning bij melding aan autoriteiten	Art. 73: meldplicht ernstige incidenten
Model- en software-updates	Release notes, compatibiliteit, regressietests, rollback-mogelijkheden	Art. 83: substantiële wijziging
Subverwerkers/keten	Transparantie over subleveranciers; contractuele flowdown van verplichtingen	Art. 25, 26: waardeketen

Tabel 9 Contractuele minimumclausules

5.2 AI Act: verantwoordelijkheden in de waardeketen

De AI Act maakt expliciet dat verantwoordelijkheden in de keten kunnen verschuiven. In bepaalde situaties wordt een distributeur, importeur of gebruiksverantwoordelijke zelf als aanbieder beschouwd, bijvoorbeeld wanneer hij een substantiële wijziging aanbrengt of het beoogd doel wijzigt. Dit maakt sourcingkeuzes en contractuele afspraken cruciaal: een ogenschijnlijk "afgenomen" AI-component kan door lokale configuratie of doelwijziging alsnog aanbiederverplichtingen triggeren.

5.3 Leveranciersmanagement: strategische sturing

Leveranciersmanagement (richtinggevend niveau) richt zich op generiek leveranciersbeleid, raamcontracten en strategische keuzes over verantwoordelijkheden. Voor AI omvat dit onder meer: keuze voor type dienstverlening (model, API, volledige dienst), allocatie van risico's, eisen aan toegankelijkheid en security, en de mate waarin leveranciers resultaatverantwoordelijk zijn voor compliance-producten. Hiermee worden kaders geformuleerd waarbinnen Contractmanagement op sturend niveau concrete afspraken maakt.

5.4 Tussenconclusie

AI-compliance stopt niet bij de grenzen van de eigen organisatie. Omdat veel AI-functionaliteit wordt afgenomen via SaaS-oplossingen, cloud-AI, API's, generieke modellen of geïntegreerde leveranciersdiensten, moet de AI-waardeketen expliciet worden beheerst. Hoofdstuk 5 laat zien dat Contractmanagement en Leveranciersmanagement hiervoor twee complementaire aangrijpingspunten bieden. Contractmanagement borgt concrete afspraken over documentatie, logging, auditrechten, incidentmelding, updates en ondersteuning bij toezicht.
Leveranciersmanagement zorgt voor kaders rond sourcing, leverancierselectie, risicotoedeling en strategische afhankelijkheden.
Daarmee wordt de evidence supply chain uitgebreid naar de externe keten. Leveranciers leveren niet alleen technologie, maar ook een deel van de bewijsvoering die nodig is voor passend gebruik, monitoring, transparantie en verantwoording. De gebruiksverantwoordelijke organisatie blijft echter verantwoordelijk voor toepassing in de eigen context. Hoofdstuk 6 brengt deze elementen samen in een integraal operating model en een roadmap voor structurele verankering in governance en interne control en audit.

6. Integrale AI-implementatie en roadmap

6.1 Koppeling aan interne controle en audit

De waarde van de evidence supply chain wordt pas volledig zichtbaar wanneer zij aansluit op bestaande interne controle-mechanismen. Het Three Lines Model (IIA, 2020)[14] biedt een bruikbaar referentiekader:

- De eerste lijn — proceseigenaren en operationeel management — draagt primaire verantwoordelijkheid voor AI-inzet en de dagelijkse uitvoering van beheersmaatregelen. Binnen BiSL zijn dit de systeemeigenaar, de informatiemanager en de functioneel beheerder. Zij produceren de operationele bewijsvoering: use case-dossiers, meldregisters, logging, monitoringrapportages en contractdossiers.
- De tweede lijn — compliance, privacy, legal en risicomanagement — stelt de normenkaders, toetst de kwaliteit van de bewijsvoering en bewaakt dat AI-inzet binnen de geldende beleids- en wettelijke kaders blijft. Zij gebruiken de BiSL-producten als input voor risicorapportages en compliance-oordelen.
- De derde lijn — interne audit — toetst onafhankelijk of de eerste en tweede lijn hun rol effectief vervullen. Bijlagen A en B zijn primair ontworpen als auditinstrument.

AI-governance wordt structureel wanneer zij onderdeel is van de reguliere P&C-cyclus: een jaarlijkse AI-governance review als vast agendapunt in de managementrapportage, kwartaalrapportages over monitoring en meldingen, en een jaarlijkse herbeoordeling van het AI-register en de risicoclassificaties.

6.2 Operating model: “AI in de lijn, compliance in de keten”

Een werkbaar operating model positioneert AI-verantwoordelijkheid in de lijn (proceseigenaren, systeemeigenaren, BIM) en organiseert compliance als keten van processen en producten. Met als kernrollen:

Rol	Verantwoordelijkheid	Positie (Three Lines)
Systeemeigenaar / proceseigenaar	Eindverantwoordelijk voor doel en risico-acceptatie in de business	Eerste lijn
(Business) informatiemanagement / functioneel beheer	Regie op use case-dossier, specificaties, acceptatie, monitoring evidence	Eerste lijn
Security / Privacy / Legal	Normenkader, toetsing DPIA/FRIA, incidentafhandeling, contractuele eisen	Tweede lijn
IT-dienstverlener(s)	Technische realisatie, documentatie, operationele logging en monitoring	Eerste lijn (uitvoering)
Interne auditor	Onafhankelijke toetsing van governance en evidence supply chain	Derde lijn

Tabel 10 Kernrollen

[14] Het Three Lines Model (voorheen Three Lines of Defense) van het IIA (Institute of Internal Auditors) is een raamwerk voor risicomanagement en governance. Het verdeelt verantwoordelijkheden in drie lijnen om de organisatie 'in control' te krijgen. Lijn 1 (business) beheert risico's, lijn 2 (compliance/risicobeheer) ondersteunt en bewaakt, en lijn 3 (audit) biedt onafhankelijke zekerheid

6.3 Roadmap in vier fasen

Onderstaande tabel vat een pragmatische roadmap samen. De fasering kan parallel lopen met de toepassingsdata van de AI Act[15] (o.a. verboden praktijken eerder van toepassing, algemene toepassing later).

Fase	Doel	Kernactiviteiten (BiSL-verankerd)	Belangrijkste deliverables
0. Baseline & mobilisatie (0–3 mnd)	Weten waar je staat	Inventarisatie AI-toepassingen; Quickscan risico; inrichten governance	AI-register; classificatie-overzicht; AI-beleid v0; RACI
1. Use case control (3–6 mnd)	Controle op nieuwe inzet	Use case-dossier als standaard (Specificeren); besluitgates (Wijzigingenbeheer); meldproces	Sjablonen; besluitvormingslog; minimale logging/monitoringset
2. Data & leveranciers (6–12 mnd)	Evidence supply chain sluiten	Data provenance; data-contracten; contractclausules; supplier due diligence	DAP/SLA-addendum AI; dataregister; audit-rights; incidentprocessen
3. Continual compliance (12+ mnd)	Structurele kwaliteit & audits	KPI's; monitoring; periodieke herbeoordeling; portfoliosturing en lifecycle-beleid	Auditrapportages; drift-reviews; verbeterbacklog; geactualiseerd beleid

Tabel 11 Roadmap in vier fasen

6.4 Tussenconclusie

AI Act-compliance wordt pas effectief wanneer beleid, processen, rollen en bewijsvoering als één samenhangend besturingsmodel functioneren. Hoofdstuk 6 laat zien hoe AI-beleid, use case-dossiers, datagovernance, monitoring, logging, leveranciersafspraken en auditbare producten worden samengebracht in een integraal operating model. De kern is dat AI-verantwoordelijkheid in de lijn wordt belegd, terwijl compliance wordt georganiseerd als een keten van processen, rollen en bewijsstukken.
De roadmap in vier fasen maakt deze inrichting praktisch uitvoerbaar: eerst overzicht via het AI-register en risicoclassificatie, daarna beheersing van nieuwe AI-initiatieven via use case-dossiers en besluitgates, vervolgens borging van datagovernance en leveranciersafspraken, en tot slot structurele continual compliance via monitoring, herbeoordeling, audits en verbeteracties.
Hoofdstuk 7 bouwt hierop voort met de centrale conclusie dat BiSL geen juridisch alternatief voor de AI Act is, maar wel een praktisch en auditbaar organisatieraamwerk om AI Act-verplichtingen aantoonbaar te operationaliseren.

[15] De toepassingsdata zijn in beweging door de standaardisatie-/Digital Omnibus-discussie. De Commissie vermeldt inmiddels dat de laatste toepassingsdatum voor bepaalde hoog-risico-regels kan liggen op 2 december 2027 respectievelijk 2 augustus 2028. Zie voor meer informatie Timeline for the Implementation of the EU AI Act | AI Act Service Desk en de EUR-Lex website Regulation - EU - 2024/1689 - EN - EUR-Lex

7. Conclusies en aandachtspunten

De AI Act maakt verantwoord AI-gebruik een expliciete compliance-plicht. De centrale conclusie van dit whitepaper is dat BiSL en de AI Act complementair zijn: de AI Act specificeert het normatieve wat, BiSL levert het organisatorische hoe. Compliance ontstaat niet uit een eenmalig juridisch traject, maar uit een keten van beleid, besluitvorming, specificatie, contractering en continue beheersing. Een evidence supply chain die in de dagelijkse besturing van de informatievoorziening is ingebed.

#	Aandachtspunt	Fase	Inspanning	BiSL-anker
1	Maak AI expliciet onderdeel van de BIM-scope: stel een AI-register in en koppel use cases aan systeemeigenaarschap	Fase 0	Laag	Behoeftemanagement, Portfoliomanagement
2	Richt governance en rollen in via RACI: benoem systeemeigenaren en leg het escalatiepad vast	Fase 0	Laag	Strategie inrichting IV-functie
3	Standaardiseer het AI-use case-dossier binnen Specificeren; differentieer voor hoog-risico vs GPAI	Fase 1	Midden	Specificeren, Wijzigingenbeheer
4	Borg AI Act Quickscan als vaste stap in Wijzigingenbeheer, inclusief herbeoordeling bij doelwijziging	Fase 1	Laag	Wijzigingenbeheer
5	Veranker DPIA/FRIA als go/no-go criterium bij hoog-risico AI; verplicht voor publieke instellingen	Fase 1	Midden	Toetsen en testen, Voorbereiden transitie
6	Sluit de evidence supply chain via Contractmanagement: documentatie, logging en auditrechten contractueel vastleggen	Fase 2	Midden	Contractmanagement
7	Implementeer de AI Data & Monitoring Control Set; gebruik Bijlage B als auditeerbare checklist	Fase 2	Hoog	Beheer bedrijfsinformatie, ILM
8	Richt monitoring en meldprocessen in voor continual compliance; koppel aan de P&C-cyclus	Fase 3	Midden	Gebruikersondersteuning, Planning & Control
9	Koppel AI-governance aan het Three Lines Model en interne audit; borg een jaarlijkse AI-governance review	Fase 3	Laag	Planning & Control, Bijlagen A en B

Tabel 12 Aandachtspunten

Minimale compliance set: aanbevelingen 1, 2, 3 en 4. Uitvoerbaar binnen fase 0–1 met beperkte extra inspanning.
Volwassen governance set: aanvullend aanbevelingen 5–9; het niveau waarop het paper volledig als referentiekader kan worden gebruikt richting externe toezichthouders.

Referenties

Juridische bronnen

1. Verordening (EU) 2024/1689 — AI Act. Europees Parlement en Raad, 13 juni 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 / https://artificialintelligenceact.eu/ai-act-explorer/ [Kernbron]
2. Verordening (EU) 2016/679 — AVG (GDPR). Europees Parlement en Raad, 27 april 2016. [Relevant voor DPIA/FRIA-relatie]. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679
3. EU AI Act — Tijdlijn toepassingsdata. Timeline for the Implementation of the EU AI Act | AI Act Service Desk

Frameworks en standaarden

4. BiSL® — Een framework voor business informatiemanagement, 4de editie. Van Haren Publishing, 2024. ISBN: 9789401811460 (printversie)
5. ISO/IEC 42001:2023 — Information technology - Artificial intelligence (AI) - Management system. International Organization for Standardization.
6. NIST AI Risk Management Framework (AI RMF 1.0). NIST AI 100-1, januari 2023 https://doi.org/10.6028/NIST.AI.100-1
7. IIA Three Lines Model. Institute of Internal Auditors, 2020; 2024 Three Lines Position Paper - IIA Sept. 2024 Update

Guidance en richtsnoeren van wetgevers en toezichthouders

8. EU AI Office — Guidelines on AI system definition. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application
9. EU AI Office — Draft Commission guidelines on the classification of high-risk AI systems. https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-classification-high-risk-ai-systems . [Kernbron]
10. EU AI Office — Guidelines for providers of general-purpose AI models. https://digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers
11. EU AI Office — Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act
12. ENISA — Cybersecurity of AI and Standardisation. European Union Agency for Cybersecurity, 2023 https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation
13. Autoriteit Persoonsgegevens — AI-verordening. https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/ai-verordening
14. Rijksoverheid — Implementatiekader 'Verantwoorde inzet van algoritmen'. Implementatiekader 'Verantwoorde inzet van algoritmen' | Rijksoverheid.nl

Vakpublicaties en aanverwante bronnen

15. Nederlandse Orde van Register EDP-Auditors (NOREA) — Guiding Principles Trustworthy AI investigations. NOREA | Publicatie NOREA Guiding Principles Trustworthy AI Investigations update

Bijlage A. Mapping BiSL-processen ↔ AI Act-verplichtingen

BiSL-proces	Primaire compliance-bijdrage	Typische producten
Gebruikersondersteuning	Signalen uit gebruik; incidenten; gebruikerscommunicatie	AI-meldingenlog; incidentrapport; FAQ/werkinstructies; escalatieregels
Specificeren	Beoogd doel, gebruikscontext, acceptatiecriteria	AI-use case-dossier; PvE; test- en acceptatiecriteria
Wijzigingenbeheer	Besluitvorming, prioritering, herbeoordeling bij wijzigingen	AI Act Quickscan; besluitlog; release-kalender; herclassificatiebesluiten
Richtinggevende processen	Kaders, prioritering, kwaliteitssturing (incl. compliance)	AI-beleid; kwaliteitsnormen; portfolio-prioriteiten; AI-register
Contractmanagement	Contractuele borging in de waardeketen	SLA-addendum AI; DAP; audit-rechten; incidentclausules
Leveranciersmanagement	Strategisch leveranciersbeleid en raamcontracten	Leveranciersbeleid; raamcontracten; sourcingstrategie
Informatie-lifecyclemanagement	Lifecycle-beleid voor AI-objecten, data, modellen	Lifecycle-beleid; classificatiekader; retentiebeleid
Beheer bedrijfsinformatie	Datakwaliteit, monitoring, compliance evidence	Datakwaliteitscorecard; issue register; compliance evidence pack
Planning & control	Bestuurlijke ritmiek en periodieke review	AI-jaarplan; reviewkalender; stuurrapportage; audittrail
Relatiemanagement gebruikersorganisatie	Competentiemanagement; verantwoordelijkheden passend gebruik	Competentiekaders; trainingsplan; communicatieplan

Bijlage B. Productenmatrix datagovernance & monitoring

#	Artefact	Owner	Doel / inhoud	Cadans	Hoog-risico
1	CDE-register (Kritieke Data Elementen)	BBI	Welke data kritiek is + eigenaar/kritikaliteit	Kwartaal + bij wijziging	A
2	Business glossary / datadefinities	BBI	Eenduidige definities & semantiek	Halfjaarlijks	A
3	Datakwaliteitsregelset + meetdefinities	BBI	DQ-regels, thresholds, meetmethode	Maandelijks	V
4	Datakwaliteit-scorecard / dashboard	BBI	KPI's, trends, drempels, uitzonderingen	Wekelijks/maandelijks	A
5	Data-Issueregister	BBI	Issues, impact, eigenaar, acties, status	Continu	V
6	Root Cause Analysis + Corrective And Preventive Action (CAPA)	BBI	Oorzaken + corrigerende/preventieve acties	Per major issue	V
7	Data lineage & dataflow map	ILM	Bron→transformatie→gebruik (incl. keten)	Halfjaarlijks + bij release	A
8	Dataset datasheet	ILM	Herkomst, populatie, representativiteit, beperkingen	Per dataset + bij wijziging	V
9	Doelbinding & use-context statement	BM	Waarvoor data/AI-gebruikt mag worden	Per use-case	V
10	Data Risk & Impact Assessment	BM	Bias/impact, ketenimpact, foutkosten, mitigatie	Per initiatief + jaarlijks	V
11	Monitoringplan	BM	Wat monitoren we, hoe vaak, wie, escalatie	Kwartaalreview	V
12	Logging policy + log retention schedule	ILM	Logscope, bewaartermijnen, toegang, integriteit	Jaarlijks + bij wijziging	V
13	Access & autorisatiematrix (data)	ILM	Rollen/rechten, reviewcyclus, least privilege	Kwartaalreview	A
14	Data classification scheme	ILM	Classificaties + maatregelen per klasse	Jaarlijks	A
15	Retention & disposal schedule	ILM	Bewaren/archiveren/vernietigen, triggers	Jaarlijks + bij wetwijziging	A

#	Artefact	Owner	Doel / inhoud	Cadans	Hoog-risico
16	Data sharing agreement (keten/extern)	BM	Delen, kwaliteit, logging, incidentmelding, auditrechten	Jaarlijks + contractwijziging	C
17	Compliance evidence pack (periodiek)	BBI	Bewijsbundel: dashboards, logsamples, reviews, Corrective And Preventive Action (CAPA)	Kwartaal/halfjaar	A

Legenda: V = Verplicht (noodzakelijk als compliance-evidence bij hoog-risico AI); A = Sterk aanbevolen; C = Contextafhankelijk (verplicht zodra de context geldt, bijv. externe data, ketens). BM = Behoeftemanagement; ILM = Informatie Lifecyclemanagement; BBI = Beheer Bedrijfsinformatie.

Bijlage C. BiSL-processen in dit whitepaper (4e editie)

Procesnaam (4e editie)	Procescluster	Primaire bijdrage aan AI-compliance	Gebruik in whitepaper
Gebruikersondersteuning	Gebruiksbeheer Uitvoerend	Meldregister AI; first-line evidence; escalatieroutes	§3.5.1, Bijlage A
Beheer bedrijfsinformatie	Gebruiksbeheer Uitvoerend	Datakwaliteitsnormen; issuebeheer; compliance evidence packs	§4.2, §4.3, Bijlage B
Operationele ketenafstemming	Gebruiksbeheer Uitvoerend	Bewaking ketenafspraken AI; signalering bij wijzigingen	§3.5.2
Operationele IT-aansturing	Gebruiksbeheer Uitvoerend	Logging, monitoring, patchstatus, retentie	§3.5.2, Bijlage A
Specificeren	Functionaliteitenbeheer Uitvoerend	AI-use-case-dossier; acceptatiecriteria; doelbinding	§3.4.2, Bijlage A
Vormgeven niet-geautomatiseerde IV	Functionaliteitenbeheer Uitvoerend	Werkinstructies; menselijke verantwoordelijkheid	§3.4.4
Toetsen en testen	Functionaliteitenbeheer Uitvoerend	Functionele en use-case tests; FRIA als go/no-go	§3.4.5
Voorbereiden transitie	Functionaliteitenbeheer Uitvoerend	Implementatieplan; autorisatiematrix; restrisico-overzicht	§3.4.6
Wijzigingenbeheer	Verbindend proces Uitvoerend	AI Act Quickscan; go/no-go besluit; herclassificatie	§3.4.1, Bijlage A
Transitie	Verbindend proces Uitvoerend	Gecontroleerde ingebruikname; overdracht naar beheer	§3.4.6
Behoeftemanagement	Sturend	Toepassings-, kwaliteits-, portfolio- en competentiekaders	§3.2, §4, Bijlagen A+B
Planning & Control	Sturend	AI-jaarplan; capaciteitsplan; reviewkalender	§3.3, §6.3
Contractmanagement	Sturend	SLA-addendum AI; DAP; auditrechten; incidentclausules	§5.1, §5.3, Bijlage A
Informatie-lifecyclemanagement	Opstellen Informatiestrategie Richtinggevend	Lifecyclebeleid AI-objecten; versie- en bewaartermijnenbeleid	§3.1, §4, Bijlage B
Informatieportfoliomanagement	Opstellen Informatiestrategie Richtinggevend	AI-portfolio; prioriteringskader; bestuurlijke besluitnota's	§3.1, Tabel 1

Procesnaam (4e editie)	Procescluster	Primaire bijdrage aan AI-compliance	Gebruik in whitepaper
Ketenpartnersmanagement	Opstellen IV-Organisatiestrategie Richtinggevend	Ketenafspraken AI; gegevensuitwisselingsprotocol	§3.1
Leveranciersmanagement	Opstellen IV-Organisatiestrategie Richtinggevend	Sourcingbeleid AI; raamcontracten; due-diligencechecklist	§3.1, §5.4
Strategie inrichting IV-functie	Opstellen IV-Organisatiestrategie Richtinggevend	AI governancemodel; RACI; rolbeschrijvingen	§3.1, Tabel 1
Informatiecoördinatie	Verbindend proces Richtinggevend	Integraal AI-beleidskader; besluitvormingskalender	§3.1

Bijlage D Twee use case-dossier voorbeelden

Hoog-risico AI — Bijlage III AI Act	GPAI-systeem — art. 51–56 AI Act
Geautomatiseerde kredietscoring voor MKB-leningen waar het gaat om kredietwaardigheid van natuurlijke personen of eenmanszaken Financiële instelling · Afdeling Zakelijk Krediet	AI-assistent voor het samenvatten en draften van beleidsdocumenten Gemeente · Afdeling Beleid en Strategie
Risicoklasse en grondslag Hoog risico Bijlage III, punt 5(b) AI Act Beoordeling van kredietwaardigheid van natuurlijke personen	**Risicoklasse en grondslag** GPAI — beperkt risico Art. 50 AI Act Microsoft Copilot ingezet via M365-licentie; geen hoog-risico classificatie
Beoogd doel en procesinbedding • AI-model genereert een kredietscore (0–1000) als input voor de kredietbeoordelaar • De beslissing tot verstrekking blijft bij een menselijke medewerker • Gebruik uitsluitend voor MKB-aanvragen tot €500k	**Beoogd doel en procesinbedding** • Ambtenaren gebruiken Copilot voor het samenvatten van raadsstukken en het genereren van eerste concepten van beleidsnota's • Output wordt altijd door een medewerker beoordeeld en bewerkt vóór gebruik • Gebruik uitsluitend voor interne beleidsontwikkeling; niet voor besluiten met rechtsgevolg
Verdeling systeem / menselijk besluit • Systeemhandelen Score + risicosignalen genereren • Menselijk besluit: goedkeuren, afwijzen, nader onderzoek	**Verdeling systeem / menselijk besluit** • Systeemhandelen: samenvatting en concepttekst genereren • Menselijk besluit: beoordelen, aanpassen, vrijgeven voor gebruik
Datakwaliteitseisen • Minimaal 36 maanden transactiehistorie aanwezig • Bias-analyse op geslacht, leeftijd en sector verplicht vóór livegang • Dataherkomstregister bijgehouden per modelversie	**Datakwaliteitseisen** • Geen vertrouwelijke persoonsgegevens als input (werkinstructie verplicht) • Documenten met classificatie "Vertrouwelijk" of hoger zijn uitgesloten van gebruik • Leverancier (Microsoft) levert dataverwerkingsovereenkomst en EU-data-residency
Acceptatiecriteria • Nauwkeurigheid ≥ 85% op validatieset • Demografische pariteit binnen 5% afwijking • Elke score voorzien van ten minste drie uitlegbare risicofactoren	**Acceptatiecriteria** • Werkinstructie "gebruik en grenzen van Copilot" beschikbaar vóór livegang • Alle gebruikers getraind op herkennen van hallucinaties en verplichte menselijke controle • Meldprocedure voor ongewenste of onjuiste output operationeel
Logging en monitoring • Input, score en uiteindelijk kredietbesluit worden gelogd • Logbewaring minimaal 5 jaar (wettelijke verplichting + AI Act min. 6 mnd) • Maandelijks drift-rapport; escalatie bij ≥ 3% afwijking	**Logging en monitoring** • Microsoft-auditlogs beschikbaar via M365 Compliance Center (minimaal 90 dagen) • Kwartaalsevaluatie gebruik en gemelde incidenten via Gebruikersondersteuning • Signalen van onjuist gebruik worden teruggekoppeld aan Behoeftemanagement

Aanvullende verplichtingen • FRIA vereist • Een conformiteitsbeoordeling • Registratie EU-database	**Aanvullende verplichtingen** • Transparantie richting gebruikers • Geen FRIA vereist • Geen conformiteitsbeoordeling
BiSL-eigenaar use case-dossier Business information manager Zakelijk Krediet	**BiSL-eigenaar use case-dossier** Business information manager Beleid en Strategie

De twee voorbeelden illustreren hoe het use case-dossier schaalt met het risicoprofiel. Bij hoog-risico AI is het dossier een formeel compliance-instrument met wettelijke verplichtingen; bij een GPAI-toepassing is het primair een organisatorisch beheersinstrument dat passend gebruik borgt. In beide gevallen is de information manager de eigenaar en is het dossier het startpunt voor zowel Toetsen en testen als Contractmanagement.