
AI Accountability: De Valkuil

Governance is niet wat u claimt.
Het is wat u kunt bewijzen.

In een omgeving van AI, toezicht en toenemende aansprakelijkheid is governance pas echt wanneer zij bewijsbaar, actueel en operationeel is. Alles daaronder is kwetsbaar voor de eerste serieuze toets.

De Apparens AI Enterprise Control Index

Acht lagen, vijf shields, acht verplichte artefacten. Vrij beschikbaar voor niet-commercieel gebruik.

ADVERSARIAL REVIEW
STRATEGIC RED TEAMING

APPARENS

The *Enterprise Control* Index

EA Enterprise Architect Cross-layer integration and architecture coherence	CISO Chief Information Security Officer Security controls and AI-specific threat modelling	CDO Chief Data Officer Data governance, regulatory readiness and evidence integrity	PROC Procurement Third-party AI governance and vendor concentration risk	CFO Chief Financial Officer AI cost governance, ROI validation and CSRD reporting
---	---	--	---	--

CONTROL INDEX FORENSIC EXPOSURE

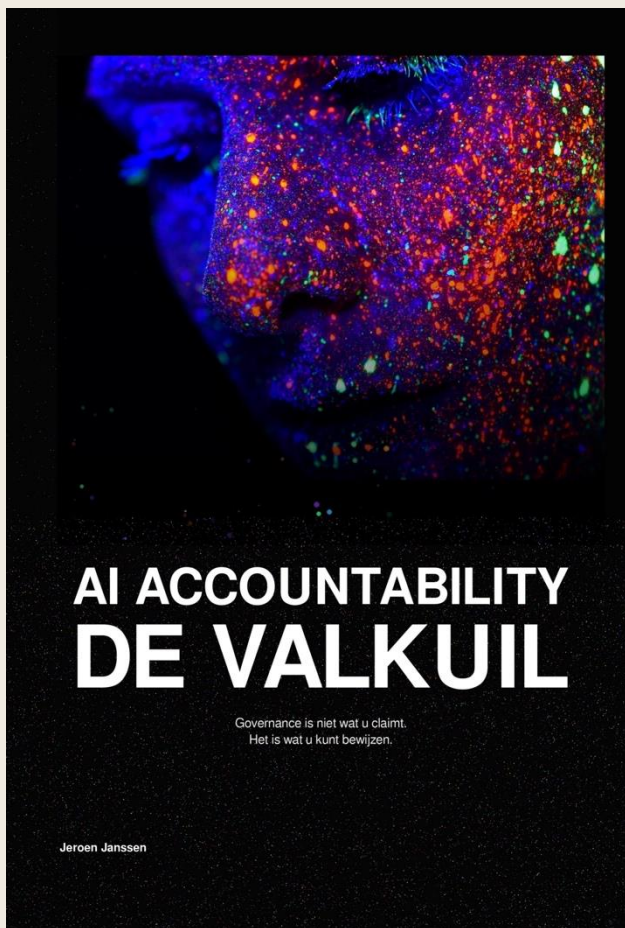
FRAMEWORK GLOSSARY BOUNDARY RULES MANDATORY ARTIFACTS STANDARDS CROSSWALK AGENTIC PACK REFERENCES

Alignment on Value

STRATEGY, ACCOUNTABILITY, ETHICS AND FAIRNESS - THE GOVERNANCE FOUNDATION EVERY AI INITIATIVE MUST SATISFY

Strategy & Accountability Mission & Public Value Ethical Principles Risk Appetite Executive Accountability AI Investment Thesis Sustainability Commitments (CSRD)	Ethics, Fairness & Accountability Bias & Fairness Testing Fairness Metrics Registry Algorithmic Auditing Process Explainability Standards Discrimination Impact Assessment Responsible AI Review Board
--	---

People & Skills ROLES, COMPETENCIES, TRAINING AND THE OPERATING MODEL FOR RESPONSIBLE AI	AI Technology Stack APPLICATIONS, AGENTS, ENGINEERING, DATA GOVERNANCE, INTEGRATION AND INFRASTRUCTURE	Control & Support Shield CROSS-CUTTING GOVERNANCE, EVIDENCE, SECURITY, COMPLIANCE AND OPERATIONAL SUPPORT
--	--	---



AI Accountability: De Valkuil

Het complete praktijkhandboek achter de
Apparens AI Enterprise Control Index.

Jeroen Janssen | Apparens
358 pagina's | 28 hoofdstukken
ISBN: 9798253336427

[Bestellen op amazon.nl](#) →

Printing on demand | Direct leverbaar
apparens.nl/book

APPARENS

Slechts een op zes organisaties rapporteert adequate AI-gereedheid.

De echte test is niet wat de organisatie zegt, maar wat zij onder druk kan tonen.

14–17%

van niet-getransformeerde organisaties rapporteert adequate AI-talent- of IT-gereedheid (AICPA/NC State 2026, n=1.735)

WAT U VANDAAG PRESENTEERT

Een framework op het intranet.
Een poster met lagen en rollen.
Een certificering op de website.
Een beleidsdocument in het archief.
Een commissie die vergadert.

Het voelt als controle.

DE VRAAG DIE HET BREEKT

Toon mij het bewijs dat control X vorige maand heeft gefunctioneerd.

Stilte.

Maar dat is geen controle.

Governance-theater ontstaat wanneer vorm aanwezig is maar bewijs ontbreekt.

Frameworks, beleid en eigenaarschap lijken controle te geven zonder operationele discipline te leveren.

De meeste governance-problemen ontstaan niet uit kwaadwillendheid, maar uit structureel verkeerd ontwerp. Vijf terugkerende faalmodi maken de valkuil systemisch voorspelbaar.

Beleidsframework

1. Adoptie zonder operationalisatie

2. Rolfragmentatie zonder integratie

3. Compliance verward met governance

4. Hoog-risico onderschatting

5. Bewijs voor auditors (niet operatoren)

Control-Framework

Afdwingbare Gates

Deployment geblokkeerd

Verplichte Artefacten

ART-01 t/m ART-08

Benoemde Eigenaren

Persoon, niet team

Actueel Bewijs

Geldigheidstermijn per artefact

Forensische Toetsing

Severity op vijf factoren

“

**Het voelt als controle en is het niet.
Dat is de illusion of control, en het verklaart waarom
governance-programma's terugglijden naar
documentatieperformance.**

”

De nieuwe vraag is niet 'wat is het plan?' maar 'kunt u het bewijzen?'

Toezicht, audit en inkoop verschuiven naar aantoonbaarheid van actuele controls en eigenaarschap.

Drie krachten convergeren en maken uitstel onmogelijk

Strategie

Geen control geldig
zonder risicobereidheid (LO)

Regulering

EU AI Act Art. 9/17
NIS2 Art. 21 | ISO 42001

Ecosysteem

Supply chain dwingt
bewijsvoering af (ART-07)

McKinsey Lilli breach | 28 februari 2026

Een autonome AI-agent brak in twee uur in bij McKinsey's interne AI-platform. Kosten: \$20 aan tokens. Resultaat: lees- en schrijftoegang tot 46,5 miljoen chatberichten, 728.000 bestanden met vertrouwelijke klantdata, en 95 schrijfbaar systeem-prompts.

Het bedrijf dat anderen adviseert over AI-governance kon de governance van zijn eigen AI-systeem niet bewijzen.

Wat het kost wanneer het misgaat

Boetes

EU AI Act: tot €35M of 7% omzet
NIS2: tot €10M of 2% omzet

License to operate

Gemeente trekt vergunning in.
Inkooppartner beëindigt contract.

Persoonlijke aansprakelijkheid

Wie tekende zonder bewijs
draagt de blootstelling.

Uw klanten en leveranciers vragen om bewijs, niet om beloftes.

Supply chain assurance dwingt governance af over grenzen, jurisdicties en contractketens heen.



Een AI-component in een gecontracteerde dienst vereist dezelfde governance als een intern systeem. Afwezigheid is contractueel risico, jurisdictieprobleem en leveranciersafhankelijkheid zonder beheersing.

De EU AI Act vereist een werkend systeem, niet een bestaand document.

Art. 9 risicomanagement, Art. 17 kwaliteitsmanagementsysteem. Beide onderscheiden werking van bestaan.

De institutionele lat is verschoven. Beleidsdocumentatie is niet langer voldoende. Toezichthouders vragen of het systeem operationeel is, niet of het beschreven is.

EU AI Act	NIS2	ISO/IEC 42001
Art. 9: doorlopend risicomanagement	Art. 21: cybersecurity incl. AI	§6.1: systematische risicobeoordeling
Art. 10: datakwaliteitsvereisten	Bestuurlijke verantwoordelijkheid	§8.4: dataprovenance
Art. 14: menselijk toezicht	Supply chain security	PDCA-cyclus
Art. 17: kwaliteitsmanagementsysteem		

“

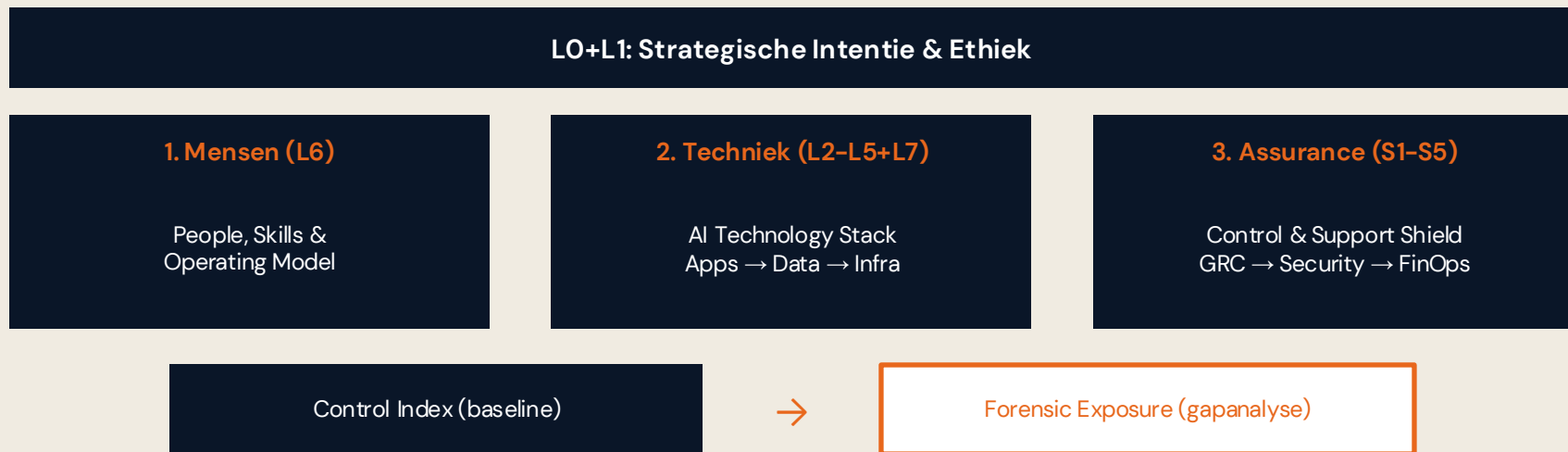
**Elke strategie wordt aangevallen.
Door regelgeving.
Door concurrenten.
Door de systemen die inmiddels sneller besluiten
nemen dan welk bestuur ook kan beoordelen.**

”

De AI Enterprise Control Index is geen beleidsframework maar een bewijsarchitectuur.

Het model is ontworpen om ontbrekend bewijs zichtbaar te maken voordat de externe toets arriveert.

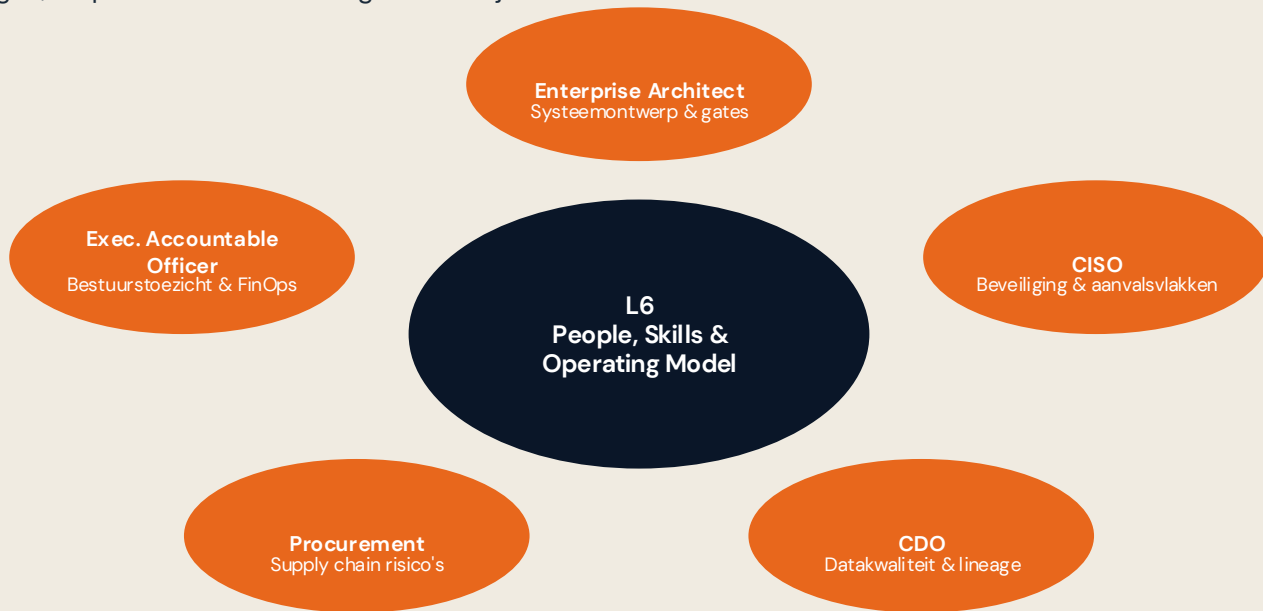
De kracht zit niet in abstracte principes, maar in de manier waarop het bewijs operationaliseert: welke controls bestaan, wie eigenaar is, welk artefact de control bewijst en of dat bewijs actueel is.



Vijf rollen dragen de discipline. Geen enkele kan het alleen.

Verantwoordelijkheid is hard gekoppeld aan specifieke functionarissen, niet aan diffuse comités.

Het rolfilter reduceert 130+ controls tot een navigeerbare werkset per rol. Elke rol heeft primaire lagen, verplichte artefacten en gates die zij moet handhaven.



Autonome agenten opereren voorbij standaard controls.

EU AI Act Art. 9 (risicomanagement) en Art. 14 (menselijk toezicht) vereisen governance die schaal met systeemautonomie.

Vanaf Autonomy Level 2 operationaliseert het framework deze verplichting via de Agent Control Declaration (ART-05). Zonder actueel ondertekende ART-05 is een opererende agent een Board-level bevinding.

ART-05 Agent Control Declaration
EU AI Act Art. 9, 14 | ISO 42001 §8.4

AGT-01 t/m AGT-07 + OWASP LLM Top 10
Zeven governance-omissies specifiek voor agentische systemen

L4: Volledig autonoom

L3: Autonoom met override

L2: Semi-autonoom

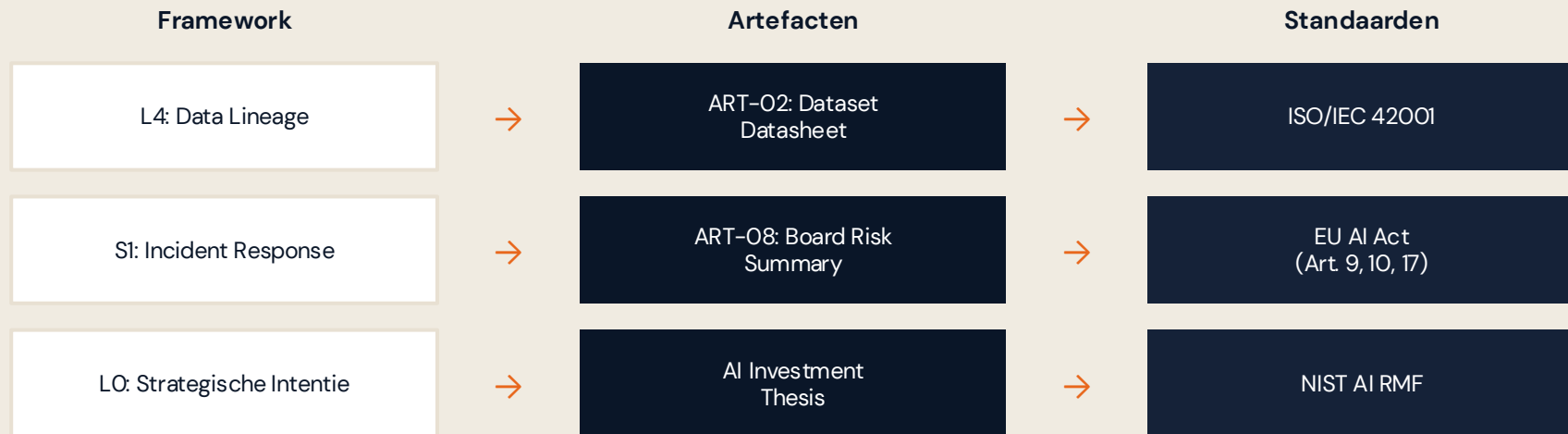
L1: Tool-assisted

VERPLICHT

U hoeft niet drie keer hetzelfde te bewijzen.

Eén set controls produceert bewijs dat meerdere regulatoire kaders tegelijk afdekt.

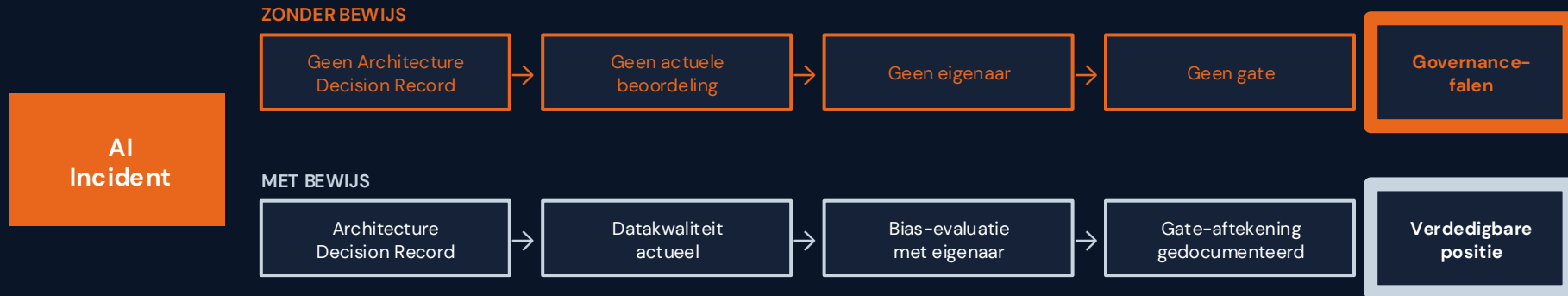
Organisaties die onder meerdere kaders opereren (EU AI Act, ISO 42001, NIST AI RMF) vrezin drievoudige bewijslast. De Standards Crosswalk lost dat op: elke control mapt naar de artikelen die hij onderbouwt. Eén bewijsinspanning, drie kaders gedekt.



Ontbrekend bewijs verschuift de schuld omhoog.

Als verantwoordelijkheden niet aantoonbaar zijn belegd, eindigt accountability bij de hoogste ondertekenaar.

Het mechanisme is consistent: incident, kritisch onderzoek, ontbrekend bewijs, escalatie naar bestuurlijke aansprakelijkheid. Wie deze sequentie begrijpt, begrijpt waarom governance bij bewijs moet beginnen.



Beleid is niet genoeg. Bewijsarchitectuur is noodzakelijk.

Acht artefacten, elk met eigenaar, trigger, gate en geldigheidstermijn. Verlopen bewijs passeert geen gate.

Een control zonder eigenaar, artefact, datum en gate is bestuurlijk zwakker dan zij lijkt.
Governance moet achterwaarts worden opgebouwd vanuit controls, artefacten, gates en eigenaarschap.

<p>ART-01</p> <p>Architecture Decision Record</p> <p>EA 12 mnd</p>	<p>ART-02</p> <p>Dataset Datasheet</p> <p>CDO 12 mnd</p>	<p>ART-03</p> <p>Model Card</p> <p>CDO 12 mnd</p>	<p>ART-04</p> <p>Risk Assessment</p> <p>EA 12 mnd</p>
<p>ART-05</p> <p>Agent Control Declaration</p> <p>EA+EAO 6 mnd</p>	<p>ART-06</p> <p>Incident Response Plan</p> <p>CISO 3 mnd*</p>	<p>ART-07</p> <p>Evidence Register</p> <p>CDO doorlopend</p>	<p>ART-08</p> <p>Board Risk Summary</p> <p>EAO kwartaal</p>

“

**Governance-claims zonder artefacten zijn beweringen.
Beweringen overleven geen regulatoire vraag, geen
inkoopuitdaging en geen incidentonderzoek.**

”

AI Accountability: De Valkuil, H2O

De kernvraag is niet of een control bestaat, maar of zij aantoonbaar actueel is.

Rapporteerbare bevindingen vereisen regulatoire grondslag, consequentiekarakterisering en benoemde verantwoordelijkheid.

Zonder alle drie is de output een mening. Meninge overleven geen regulatoire toetsing. De driedelige forensische test en vijf-factor severity-regel kwalificeren de werkelijke blootstelling.

De driedelige forensische test

- 1** **Regulatoire grondslag**
Heeft deze leemte een specifiek artikel of verplichting als haak?
- 2** **Consequentiekarakterisering**
Wat is de plausibele worst-case als deze leemte voortduurt?
- 3** **Benoemde verantwoordelijkheid**
Wie bezit de beslissing: remediëren, tolereren of escaleren?

Vijf-factor severity-regel

- 1** Regulatoire relevantie
- 2** Materialiteit van gevolgen
- 3** Systemcontext
- 4** Persistentie
- 5** Eerdere onopgeloste status

Output:

Board-level

Significant

Acceptable

Het Board Risk Summary converteert analyse naar een bestuursbesluit.

Het bestuur is geen publiek. Het is een besluitvormend orgaan. Elk overzicht sluit af met een vereiste beslissing.

Een Board Risk Summary dat afsluit met een lijst van leemten zonder governance-positie heeft zijn doel gemist. Het document moet een beslissing vragen of bevestigen dat geen nieuw besluit vereist is.

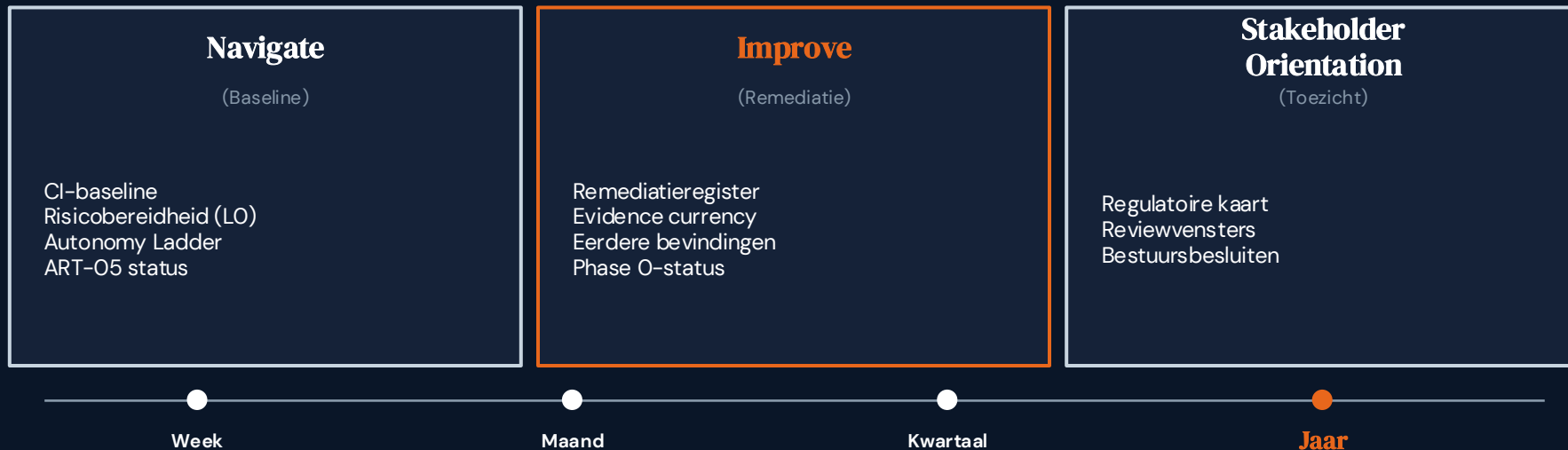


Board Risk Summary	
1. Scope	Systemen, risicoklasse, rol
2. Baseline	Present / Partial / Absent
3. Leemten	Standaard-gekoppelde blootstelling
4. Remediatie	Eigenaar, termijn, status
5. Besluiten	Vereiste bestuursautorisatie

De Governance Obeya borgt permanente zichtbaarheid.

Een gedeelde, visuele controlestructuur voorkomt terugval naar passieve documentatieperformance.

Waaraan u aandacht besteedt, groeit. Een organisatie die haar governance-status visualiseert produceert betere governance omdat leemten zichtbaar zijn, eigenaren benoemd en de cadans reactie afdwingt.



Elk hoofdstuk toont het framework in actie aan de hand van Green Canopy Ventures.

GCV is een fictieve scale-up in stedelijke bosbouw. De governance-problemen zijn dat niet.

Het boek bevat een volledig uitgewerkte casus: van auditbrief tot Board Risk Summary. Practitioners krijgen geen abstract model maar een concreet voorbeeld van elke stap, elk artefact en elke bestuursbeslissing. Inclusief het memo aan het bestuur.

Waarom een fictieve casus?

Drie AI-systemen in productie:

- Predictive Risk Scoring Agent (L2)
- Computer Vision Module (L3)
- MRV Validation Agent (L1)

Een gemeentelijke audit over 22 weken.
Nul bestaand governance-bewijs.

De details verschillen van uw organisatie.
De governance-problemen zijn dezelfde.

Wat u erin vindt

Per hoofdstuk een GCV-praktijkblok:

- Control Index-pass met scores
- Standards Crosswalk per kader
- Forensische analyse met severity
- Remedatieregister met eigenaren
- Volledig Board Risk Summary
- Bestuursbeslissingen met notulen

Kopieerbaar als template voor uw eigen governance-programma.

“

Een verdedigbare governance-positie vereist iets om te tonen, niet alleen iets om te zeggen. Controls, benoemde eigenaren en gedateerd bewijs maken het verschil.

”

Van framework naar operationele discipline in negentig dagen.

Vier strakke fasen converteren onbeheerste risico's tot audit-klare processen.

Het plan comprimeert voor startups en schaalte voor gereguleerde ondernemingen.
Weken 1-4 zijn het minimaal levensvatbare vertrekpunt.



De governance-verplichting verschilt per organisatietype. De bewijsstandaard niet.

Een startup comprimeert. Een gereguleerde onderneming kan niet bezuinigen. Een publieke organisatie coördineert.

Het Evidence Register is voor alle drie het vertrekpunt. De meeste organisaties hebben artefacten maar geen enkel overzicht van hun actualiteit.

Startup / Scale-up

ART-01, ART-03, ART-05 (als L2+)
Weken 1-4 als minimum
Focus: classificatiehelderheid
en gate-discipline

Gereguleerde onderneming

Alle acht artefacten, volle scope
Prioriteit Evidence Register
Artefacten bestaan, overzicht
van actualiteit niet

Publieke organisatie

Board Risk Summary als
primair deliverable
EU AI Act hoog-risico + ART-05
90-dagen verlenen

Governance is niet wat u claimt. Het is wat u kunt bewijzen.

Dat is niet alleen de slotzin van het boek, maar de centrale bestuurslogica eronder. Een verdedigbare governance-positie vereist iets om te tonen, niet alleen iets om te zeggen. Controls, benoemde eigenaren en gedateerd bewijs maken het verschil tussen geruststelling en aantoonbaarheid.

**Beheerste en belegde blootstelling
= Verdedigbaar en Bestuurbaar**

**Ontbrekend bewijs onder druk
= De Accountability-Valkuil**