CyberSphinx

POWERED BY THE ARGUS FRAMEWORK™

Identity-Driven AI Governance

Waarom identity het fundament is van veilige AI-adoptie

Executive Whitepaper
CyberSphinx • 2026

www.cybersphinx.nl

Inhoudsopgave

Hoofdstuk 01

Executive Summary

Artificial Intelligence transformeert organisaties in een ongekend tempo. Wat begon met experimenten en pilots is uitgegroeid tot een strategische prioriteit op boardroom-niveau. De belofte is helder: efficiëntere processen, betere besluitvorming, concurrentievoordeel.

Maar er is een fundamenteel probleem.

De meeste organisaties implementeren AI zonder het fundament op orde te hebben. Systemen zijn gefragmenteerd, verantwoordelijkheden zijn onduidelijk en er is geen zicht op wie — of wat — toegang heeft tot welke data en systemen. AI versnelt in die context geen intelligentie. Het versnelt complexiteit, risico en onbeheersbaarheid.

De ontbrekende schakel is identity.

Identity Governance bepaalt wie wat mag, wanneer en waarom. Het legt de basis voor accountability, traceerbaarheid en controle. Zonder die basis is AI-adoptie een strategisch risico. Met die basis wordt AI een strategisch voordeel.

Het ARGUS Framework™ van CyberSphinx verbindt identity, governance, security en AI tot één samenhangend operating model — een strategisch kader waarmee Europese organisaties AI veilig, gecontroleerd en soeverein kunnen adopteren.

"Trusted AI starts with trusted identities."

Hoofdstuk 02

Context — Wat is er veranderd

De AI-explosie

De adoptie van Artificial Intelligence is in een stroomversnelling geraakt. Generatieve AI, copilots, autonome agents — wat twee jaar geleden nog experimenteel was, is vandaag operationeel. Maar de governance houdt zelden gelijke tred met de adoptie.

Gefragmenteerde IT-landschappen

De meeste organisaties opereren in complexe, hybride omgevingen. Niemand weet precies wie toegang heeft tot welke systemen. Niemand weet welke AI-tools data verwerken — en op welke basis.

Nieuwe identiteiten

Het identiteitslandschap is fundamenteel veranderd:

- **Menselijke identiteiten** — medewerkers, externen, leveranciers
- **Machine identities** — service accounts, API-keys, certificates
- **AI-agents** — copilots, autonome agents, geautomatiseerde workflows

Deze niet-menselijke identiteiten groeien exponentieel en vormen inmiddels het merendeel van alle identiteiten.

Regelgeving versnelt

Europa loopt voorop. De EU AI Act, NIS2, DORA en de GDPR vereisen allemaal dat organisaties weten wie toegang heeft tot wat, dat beslissingen traceerbaar zijn en dat er eigenaarschap is ingericht.

Identity als nieuwe perimeter

De traditionele security perimeter bestaat niet meer. De nieuwe perimeter is identity. Wie je bent, bepaalt wat je mag. Wat je mag, bepaalt wat AI namens jou kan doen.

"Organisations need a new approach to AI — one that starts with identity."

Hoofdstuk 03

Het Kernprobleem

AI-adoptie versnelt terwijl het fundament ontbreekt. De technologie is beschikbaar, de druk is hoog, maar de basisvoorwaarden voor veilige inzet zijn niet op orde.

— Geen zicht op identiteiten

Dormante accounts blijven actief. Orphaned identities stapelen zich op. Service accounts zonder eigenaarschap. Dit is geen IT-probleem — het is een governance-probleem dat exponentieel versterkt wordt door AI.

AI zonder governance

AI-tools worden geïmplementeerd zonder eigenaarschap, zonder beleid, zonder kaders. Wie is verantwoordelijk als het misgaat? In de meeste organisaties: niemand.

Geen ownership van AI-agents

AI-agents handelen namens iemand — of iets. Maar in de praktijk ontbreekt die koppeling. AI opereert in een vacuüm van accountability.

Onvoldoende toegangscontrole

Least privilege wordt niet consequent toegepast. Voor AI-agents is het vaak volledig afwezig. AI krijgt brede toegang omdat het technisch eenvoudiger is.

Compliance als risico

Zonder centraal zicht op identiteiten is compliance een illusie. Audits worden reactief in plaats van proactief.

AI wordt geïmplementeerd zonder controlelaag. De organisatie versnelt in het donker.

Hoofdstuk 04

Key Insight — Identity is de Missing Layer

AI handelt altijd namens een identity

Elke AI-actie vindt plaats in een context. Een copilot die een document samenvat, doet dat namens een gebruiker. Een workflow opereert onder een service account. Die context is altijd een identity. Zonder die koppeling: geen traceerbaarheid, geen accountability, geen governance.

Zonder identity geen accountability

Wie heeft deze beslissing genomen? Op basis van welke data? Met welke bevoegdheid? Dat vereist dat elke AI-agent opereert binnen een governance-kader.

Zonder governance geen controle

Governance is het antwoord op: wie mag wat, wanneer en waarom? Identity Governance geeft dat antwoord.

De drie-eenheid van identity

Identity = Security	Wie heeft toegang? Identity-centric security maakt toegang beheerbaar, traceerbaar en revocable.
Identity = Governance	Wie is verantwoordelijk? Identity Governance borgt eigenaarschap, bevoegdheden en accountability.
Identity = Compliance	Is het aantoonbaar? Identity levert de audit trail die regelgeving vereist.

"Identity is the foundation of trusted AI."

Hoofdstuk 05

Het ARGUS Framework™

ARGUS is vernoemd naar de wachter uit de Griekse mythologie — de bewaker met honderd ogen. Het ARGUS Framework™ is een strategisch operating model dat identity, governance, security en AI verbindt — gebouwd voor Europese organisaties.

De vier pijlers

Identity Governance
Wie heeft toegang tot wat, wanneer en waarom? Het fundament van het hele model.

Security
Identity-centric security. Human identities, machine identities en AI-agents in governed environments.

AI Governance
Eigenaarschap, besluitvorming en accountability voor AI-agents en AI-gedreven processen.

Organisational Intelligence
De verbinding van alle lagen creëert organisatie-brede intelligentie.

De ARGUS-componenten

ARGUS Framework™
Het strategische operating model. De blueprint voor Identity-Driven AI Governance.

ARGUS Methodology™ (6C)
Business-driven implementatie: Check, Course, Configure, Coach, Care, Communicate.

ARGUS Maturity Model™
Zes niveaus van Unmanaged tot Autonomous Organisation.

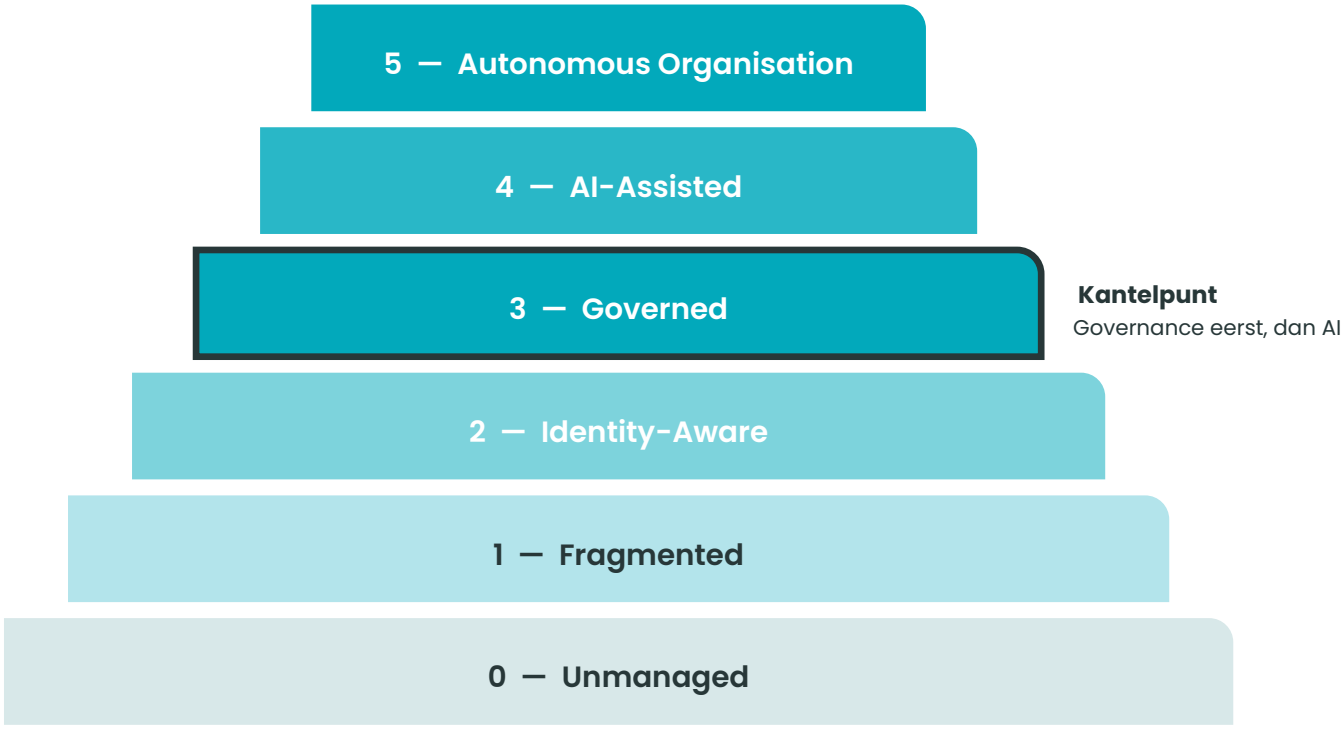
ARGUS Identity-Driven AI Compass™
Executive assessment — vijf strategische vragen, direct inzicht.

ARGUS Cybersecurity Teammate™
Continue operationele AI-intelligentie voor security teams.

Hoofdstuk 06

Het ARGUS Maturity Model™

Het ARGUS Maturity Model™ beschrijft de reis van een organisatie in zes niveaus.



Unmanaged
Geen zicht op identiteiten, geen beleid, volledig reactief.
"We weten niet wie toegang heeft tot wat."

Fragmented
Silo's, geen centraal zicht, ad-hoc toegangsbeheer.
"We hebben systemen, maar geen overzicht."

Identity-Aware
Eerste zicht op identiteiten, basis controles ingericht.
"We zien onze identiteiten, maar beheren ze nog niet volledig."

Governed
Centrale governance, policies, compliance geborgd. Dit is het kantelpunt.
"We weten wie wat mag, wanneer en waarom."

AI-Assisted
AI ondersteunt operations en governance processen.
"AI versterkt onze governance en operations."

Autonomous Organisation
Zelflerend, AI-gedreven, volledig verbonden.
"De organisatie is zelflerend, verbonden en veilig."

Belangrijk: Niveau 3 (Governed) moet op orde zijn voordat AI veilig kan worden ingezet.

Hoofdstuk 07

Praktische Toepassing

Vier scenario's — zonder technische details, maar herkenbaar voor iedere beslisser.

AI-agents met identity

Elke AI-agent opereert onder een beheerde identiteit met duidelijke bevoegdheden. Er is een eigenaar. De bevoegdheden zijn begrensd. Elke actie is traceerbaar.

Toegang gekoppeld aan governance

AI krijgt uitsluitend toegang tot de data die nodig is. Dynamisch beheerd. Verandert de rol, dan verandert de toegang. Least privilege als standaard.

Traceerbaarheid van acties

Elke stap is traceerbaar: welke data, welke regels, welke bevoegdheid. Dit is wat regelgeving vereist en wat bestuurders nodig hebben.

Compliance monitoring

Continue monitoring in plaats van periodieke audits. Identiteiten en AI-acties worden real-time gemonitord. Afwijkingen automatisch gesignaleerd.

Hoofdstuk 08

Business Impact

Identity-Driven AI Governance adresseert vijf business drivers.

Business Driver	Zonder ARGUS	Met ARGUS
Risk Mitigation	Onbeheerde identiteiten, ongecontroleerde AI-agents	Identity-centric governance. Elke identiteit beheerd, elke beslissing traceerbaar.
Security	Netwerkgerichte, reactieve security	Identity-centric security met Zero Trust en continue verificatie.
Compliance	Reactieve audits, geen structureel zicht	Continue compliance operations. Audit-readiness als standaard.
Efficiency	Teams schalen niet mee met complexiteit	Geautomatiseerde governance, AI-ondersteunde operations.
AI Enablement	AI zonder fundament = experiment	Identity als enabler van veilige, schaalbare AI-adoptie.

Hoofdstuk 09

Conclusie

AI is geen optie meer. De vraag is niet óf AI wordt geadopteerd, maar hoe.

Organisaties die AI implementeren zonder governance, bouwen op een fundament van zand.

De oplossing begint bij identity.

Identity Governance biedt traceerbaarheid, accountability en controle. Het ARGUS Framework™ maakt dit concreet — pragmatisch, Europees, gebouwd voor organisaties die AI willen benutten zonder controle te verliezen.

De organisaties die nu investeren in dat fundament, zullen AI als strategisch voordeel inzetten. De rest zal blijven worstelen.

"AI with identity governance becomes a strategic advantage."

ARGUS IDENTITY-DRIVEN AI COMPASS™

Ontdek waar uw organisatie staat

Vijf strategische domeinen:

1. **Identity Ownership**
2. **Governance & Accountability**
3. **Security & Risk Management**
4. **AI Governance & Usage**
5. **Organisational Intelligence**

Twee minuten. Geen voorbereiding. Direct inzicht.

Start de ARGUS Compass™

www.cybersphinx.nl/argus-compass

Persoonlijk gesprek?

www.cybersphinx.nl/contact

www.cybersphinx.nl