

# ANDRÉS LAGE FREIRE

Responsible AI Architect | AI Governance & AI Assurance

Based in Madrid · Working remotely across EMEA

+34 605 45 92 45 · andreslage@tshapedconsultant.com · tshapedconsultant.com · GitHub · LinkedIn

## EXECUTIVE SUMMARY

Responsible AI Architect and Strategic AI Governance Lead specialized in helping organizations transform AI initiatives from proof-of-concept into governed, auditable and scalable systems. Operating at the intersection of business, engineering, cybersecurity, legal and compliance functions, I establish AI Governance operating models, risk management frameworks and Responsible AI controls aligned with the EU AI Act, ISO/IEC 42001 and NIST AI RMF — translating regulatory obligations into executable controls, SDLC gates and runtime assurance.

### SPECIALIZED IN

|                     |                            |                         |
|---------------------|----------------------------|-------------------------|
| AI Governance       | Responsible AI             | Agentic AI Governance   |
| EU AI Act Readiness | ISO/IEC 42001              | AI Risk Management      |
| AI Assurance        | Enterprise AI Architecture | AI Lifecycle Governance |

## SELECTED AI GOVERNANCE PROJECTS

### Enterprise AI Vendor Governance Console

[github.com/tshapedconsultant/enterprise-ai-risk](https://github.com/tshapedconsultant/enterprise-ai-risk)

#### STACK · V1.4.0

- Deterministic scoring · GDPR + EU AI Act + ISO/IEC 42001 + NIST AI RMF
- Jira human gates · hash-chained audit (Jira/Rekor/S3)
- FastAPI · Pytest · Docker · CI

**Outcome.** Executable vendor risk controls: deterministic rules engine with HMAC-validated webhooks, external audit anchoring, and CI-deployed evidence packs.

### Responsible AI Compliance Hub

[github.com/tshapedconsultant/porto-seguro-compliance-hub](https://github.com/tshapedconsultant/porto-seguro-compliance-hub)

#### DATASET · 595K RECORDS

- EBM glass-box classifier · Polars ingestion
- KS drift gates · fairness audits (Art. 9, 14, 15)
- JSON evidence packs · Solvency II conformity · FastAPI · Streamlit

**Outcome.** Five-layer reference architecture mapping EU AI Act Articles 9–15 to executable controls; demonstration model achieved ROC-AUC 0.64.

### Enterprise Data Analyst Agent

OpenAI-powered governed multi-agent architecture for enterprise reporting

#### FOCUS

- Agentic AI
- Human oversight
- Auditability
- Enterprise controls

**Outcome.** Demonstrated agentic systems designed with accountability, traceability and control-by-design principles.

### tshapedconsultant.com — AI Governance Engineering website

[tshapedconsultant.com](https://tshapedconsultant.com)

#### 2026 · AI-ASSISTED ENGINEERING

- Built end-to-end with Cursor and LLM-assisted coding
- Mobile-first UX · accessible navigation · responsive evidence mapping
- Governance-artifact framing: EU AI Act controls, evidence packs, reference implementations

**Outcome.** Primary consulting presence and portfolio artifact demonstrating AI-augmented engineering capability.

Additional work. AI Red Team Orchestrator — Azure-hosted GARAK framework for AI assurance and adversarial testing; created reusable assurance patterns to evaluate robustness and readiness before deployment.

## PROFESSIONAL EXPERIENCE

### Strategic AI Consultant & Responsible AI Architect (Independent)

Jun 2021 – Present

International · Jun 2021 – Present

#### RESPONSIBLE AI & STRATEGY

- Created DGOM™, a Board-to-Code AI risk operating model translating regulatory obligations, risk appetite and executive decisions into executable controls, SDLC gates, runtime assurance and auditable evidence.
- Established Human-in-the-Loop (HITL), escalation and dual-approval patterns for high-impact AI decisions; benchmarked risk operating models from Microsoft, Deloitte and BBVA.

#### APPLIED AI ARCHITECTURE & TECHNICAL LEADERSHIP

- Architected governed multi-agent AI prototypes using LangGraph, FastAPI and OpenAI API with control-by-design principles.
- Designed controls-first ML pipelines integrating explainability, bias monitoring, drift detection and tamper-evident audit logging using PyTorch, TensorFlow and Scikit-learn.
- Designed AI deployment patterns across AWS Bedrock, Azure OpenAI and Databricks for scalable inference and analytics.

- Stakeholder Leadership. Acted as trusted advisor between engineering, compliance, cybersecurity, legal and executive stakeholders.

### Cloud Implementation Specialist — Avaya Cloud Office

Oct 2020 – Jun 2021

Concentrix · Sofia, Bulgaria

- Led cloud deployment projects for multinational enterprise clients under strict security and compliance requirements.
- Acted as primary interface between technical delivery teams and executive stakeholders; streamlined rollout processes for multinational enterprise clients.

### Innovation Project Lead (Award Winner)

2018

Repsol Foundation · 2018

- Led the team awarded the Repsol Foundation Entrepreneurship Prize.
- Applied Lean experimentation and business validation methodologies with corporate partners.

## CORE COMPETENCIES

| AI GOVERNANCE & RISK                                                                                                                                                                                                          | AGENTIC AI & LLM ENGINEERING                                                                                                                                                                                 | ML/DL ENGINEERING                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• EU AI Act</li><li>• ISO/IEC 42001</li><li>• NIST AI RMF</li><li>• AI Risk Assessment</li><li>• Human-in-the-Loop Governance</li><li>• AI Assurance</li><li>• AI Red Teaming</li></ul> | <ul style="list-style-type: none"><li>• Multi-Agent Systems</li><li>• LangGraph</li><li>• LangChain</li><li>• RAG Architectures</li><li>• OpenAI API</li><li>• Azure OpenAI</li><li>• GARAK</li></ul>        | <ul style="list-style-type: none"><li>• PyTorch</li><li>• TensorFlow</li><li>• Scikit-learn</li><li>• Model Deployment</li><li>• FastAPI</li><li>• Monitoring &amp; Validation</li></ul> |
| CLOUD, DATA & MLOPS                                                                                                                                                                                                           | SECURITY, TRUST & COMPLIANCE                                                                                                                                                                                 | LEADERSHIP                                                                                                                                                                               |
| <ul style="list-style-type: none"><li>• Python</li><li>• SQL</li><li>• Docker</li><li>• Kubernetes</li><li>• AWS Bedrock</li><li>• Databricks</li><li>• Azure AI Services</li></ul>                                           | <ul style="list-style-type: none"><li>• GDPR</li><li>• AI Compliance</li><li>• Explainability (SHAP, LIME)</li><li>• Prompt Injection Defense</li><li>• Vendor Risk</li><li>• Tamper-evident Audit</li></ul> | <ul style="list-style-type: none"><li>• Executive Communication</li><li>• Stakeholder Alignment</li><li>• Strategic Advisory</li><li>• AI Lifecycle Transformation</li></ul>             |

## EDUCATION & CREDENTIALS

### Harvard SEAS

2026

Agentic AI Foundations: Business Applications and Risks

### Stanford Online

2026

Cybersecurity and Executive Strategy (XACS302)

### Oxford Saïd · UNESCO

2026

AI, Justice, and the Rule of Law

### IAPP AIGP

2026

Examination scheduled 30 November 2026 · Certification in progress

### Oxford — Saïd Business School

2025

AI Governance Programme

### Wharton

2025

AI Strategy & Governance

Independent AI Governance and AI Systems Research Programme (2025–Present) — Self-designed curriculum validated through implementation and comparative research, spanning AI governance, agentic AI, ML/MLOps, cybersecurity, privacy, and responsible AI.

Additional programmes. Harvard Online — Innovation Strategy · Stanford — Advanced Learning Algorithms, AI Awakening · Michigan — Responsible Generative AI · Yale — Narrative Economics.

### Chemical Engineering (Plan Superior)

2002–2008

IQS School of Engineering – Universitat Ramon Llull · 2002–2008 · 247.5 ECTS