US East, Where Systems Build Success

John D'Esposito

SUMMARY

AI Governance and Responsible AI leader with **20+ years** of experience in technology governance, risk management, and large-scale enterprise systems, including recent deep focus on AI/ML and LLM governance.

Proven ability to design and operationalize end-to-end AI governance frameworks—translating regulatory and ethical requirements (**ISO 42001, NIST AI RMF, EU AI Act, PHI/PII**) into enforceable technical controls, model oversight workflows, and continuous monitoring across the full AI lifecycle.

Known for building governance that executes: policy-driven, auditable, and resilient AI systems aligned with Legal, Privacy, Security, Engineering, and Compliance stakeholders.

CORE AI GOVERNANCE DOMAINS

- AI Governance Strategy & Operating Models
- Responsible AI (Fairness, Bias, Explainability)
- AI / ML / LLM Risk Management
- Model Oversight, Inventory & Accountability
- AI Lifecycle Gov. (Design → Deploy → Monitor)
- LLM Cost Controls
- LLM Traffic Management
- AI Data Factory
- PII / PHI Detection, Sanitization & Data Protection
- AI Observability, Drift & Misuse Detection
- Regulatory Alignment (NIST AI RMF, ISO 42001, EU AI Act)
- Cross-Functional Governance Leadership
- Policy Documentation & Risk Registers
- Data Bricks
- Snowflake

GOVERNANCE & CONTROL CAPABILITIES

- **AI Risk Identification & Mitigation** – Data sensitivity classification, prompt inspection, risk-tiering, and policy-based model routing to prevent regulatory and ethical violations before execution.
- **Responsible AI Enforcement** – Bias exposure reduction, explainability hooks, prompt governance, and restricted model usage enforced at runtime—not left to application code.
- **Model Oversight & Accountability** – Model inventories, access controls, audit logging, governance dashboards, Model Cards, Data Sheets, and Risk Registers.
- **Continuous Monitoring & Drift Detection** – Real-time monitoring of AI behavior, cost, security posture, and compliance signals across production environments.

TECHNICAL SKILLS

AI Traffic & Prompt Governance	Kong AI Gateway, Kagent AI Gateway, Risk-Aware LLM Routing, Prompt Sanitization, Microsoft Presidio
AI/ML Lifecycle & Observability	Dynatrace, Kong Konnect, Kagent AI Gateway
Governance Automation	Kong AI Gateway, Kagent AI Gateway, Kong Konnect, Custom LUA AI Plugins, Custom MCP Servers, Custom MCP Bridge, Custom MCP Oauth, n8n,, OPA Policies, Claude Desktop, Claude Code, Gemini, NotebooLM, Bedrock, AWS Sagemaker, Perplexity, OpenAI, Snowflake, Data Bricks, AI Data Factory
Cloud & Infrastructure	Terraform & Terragrunt Infrastructure as Code, AWS CloudFormation Automation, Multi-Cloud Infrastructure (AWS, Azure, GCP), Kubernetes Platform Automation (EKS / AKS / GKE), CI/CD-Driven Infrastructure Pipelines, GitHub Actions & GitHub Workflows, Azure DevOps Infrastructure Pipelines, GitOps-Based Environment Management, Secure IAM & RBAC Automation, Policy-Aware Infrastructure Deployment

EXPERIENCE

AI Governance Architect | Securing Enterprise AI
Amalfi AI **Sep 2024 – Present**

Building AI Governance frameworks that prevent breaches, ensure compliance, cut costs, and centralize observability. Transforming ungoverned AI into secure, compliant, policy-driven operations.

Responsibilities and Deliverables:

- **Risk-Aware LLM Routing Plugin Development** – Architecting Kong AI Gateway plugins where prompts are dynamically classified (PII, IP, regulatory sensitivity) and routed to appropriate models before execution. Moves AI governance from application code into centralized control plane, transforming LLM usage from best-effort into auditable, policy-driven system.

- **End-to-End AI Governance Frameworks** – Design and implement comprehensive governance from board policies to technical controls. Deploy automated compliance for HIPAA/GDPR/SOC2/PCI with full audit trails. Create governance dashboards showing real-time risk, costs, and compliance status.

- **AI Security & Prompt Sanitization** – Build multi-layer pipelines detecting and blocking PII/PHI before reaching LLMs using Microsoft Presidio and AWS Comprehend. Deploy prompt injection defenses achieving 99.8% effectiveness. Implement zero-trust architectures with complete audit trails.

- **Model Oversight & Accountability** – Establish model inventories, access controls, audit logging, and governance dashboards. Create Model Cards, Data Sheets, and Risk Registers for AI/ML lifecycle governance from design through deployment and monitoring.

- **Custom MCP Server Development** – Develop governance-aware MCP servers extending Claude for enterprise needs. Build compliance-aware document processing tools and industry-specific servers (legal, healthcare, financial) integrated with enterprise systems.

- **n8n Workflow Automation** – Architect intelligent workflows replacing manual AI operations. Build automated incident response for security events and compliance reporting with 24/7 policy enforcement.

Recent Impact:

- Healthcare: HIPAA-compliant MCP server preventing 2.3M PII leakage attempts
- Financial Services: Saved client $1.2M in potential GDPR fines via governance + n8n automation
- Fortune 500: Blocked 99.8% prompt injections while cutting AI costs 52%

Technologies: Kong AI Gateway, Solo.io AI Gateway, AWS Bedrock, AWS Sagemaker, Data Bricks, Snowflake, AI Data Factory

ApiOps, MLOps, AI Traffic Mgt, AI Governance Engineer
Blackstone **Jun 2020 – Sep 2024**

Senior Cloud DevOps Architect responsible for advancing strategic AI governance initiatives and implementing cloud-based automation for major API transformation serving 7B+ daily requests.

Responsibilities and Deliverables:

- **AI Governance, AI Observability, AI Security, AI Traffic Management** – Introduced Kong AI Gateway as AI proxy with multiple AI services, normalizing APIs and providing decoupled inference format. Implemented prompt templating for guided AI usage and prompt protection using regex-based prompt engineering at gateway level. Built centralized/unified AI observability, security, and performance management with third-party LLM integrations.

- **LUA Plugin Development** – Authored custom LUA plugins for Kong Gateway handling special authorization use cases, prompt validation, and traffic routing logic.

- **API Management Strategy - Kong Konnect / API Gateway** – Implemented Kong API Gateway through Kong Konnect using AWS ECS Fargate supporting 7 billion+ daily mobile requests. Fully automated through Terraform across multiple AWS availability zones.

- **AI Ops and Observability** – Designed observability approach for continuous health monitoring using Kong metrics, Grafana, Prometheus, OpenTelemetry, and Dynatrace. Leveraged Dynatrace AI to detect, isolate, and determine root cause of performance issues.

- **Service Mesh - Kong Mesh** – Implemented cross-region multi-service API authentication, authorization, security, and traffic control using Kong Service Mesh with Kuma/Envoy sidecars.

DevOps & Automation Architect
Goldman Sachs – Apple Card **Feb 2018 – Jun 2020**

DevOps Architect responsible for infrastructure and applications supporting high-volume, customer-facing banking transactions for Apple Card across multi-account, multi-region environments.

- **Compliance as Code** – Introduced technologies enabling enterprise to manage compliance as code, automatically inspecting infrastructure and services for security and configuration compliance. Automated CIS Level 1 security testing with Goldman Sachs Tech Risk requirements.

- **Secrets Management & Security** – Deployed enterprise-class static and dynamic secrets management using Hashicorp Vault and Consul. Worked with Tech Risk teams to continuously detect and remediate security risks.

Technologies: Python/boto3, Ansible, Hashicorp Terraform/Vault/Consul, AppDynamics, AWS Services, Inspec

ADDITIONAL EXPERIENCE

Liberty Mutual Insurance | ***DevOps & Automation Architect*** **Jun 2017 – Feb 2018**
Designed DevOps toolchain enabling mission-critical systems deployment in AWS EC2 with compliance as code and secrets management.

GE Digital | ***DevOps & Automation Engineer*** **Sep 2016 – Jun 2017**
Automated secure configuration of Predix Appliance meeting US/International GE security standards using Inspec framework for audit controls.

Earlier: Raymond James, News Corp/Dow Jones, GE Capital, NY Federal Reserve, JPMorgan Chase, IBM - (12 years)

Industries: Healthcare (HIPAA), Financial Services (PCI/SOX), Insurance, Airlines, Government, E-commerce (GDPR)

CERTIFICATIONS & PATENTS

- ServiceMesh Certification
- Advanced Dynatrace Certification
- Patent: Remote and Real-Time Network and HTTP Monitoring With Real-Time Predictive End User Satisfaction Indicator (US 8972569)
- Patent: System and Method For Clustering Servers for Performance and Load Balancing (US 6965938)
- Patent: Method and Computer Program for Web Site Performance Monitoring and Testing (US 2006/0020699)

PUBLICATIONS

- Creating an Effective DevOps Strategy
- Creating ChatOps & Incident Response Solutions

EDUCATION

Lafayette College, Easton PA
Bachelor of Science, Electrical Engineering