AI/LLM Security Governance & Risk Assessment

Empower your organization to adopt Large Language Models (LLMs) and agentic AI safely with proactive governance, risk modeling, and security validation.

Service Overview

Our comprehensive vCISO-led service helps organizations secure AI systems through integrated governance, AI-specific threat modeling, detection tuning, and targeted red-team validation. The goal: build confidence, compliance, and resilience in every AI deployment.

Core Service Components

AI Governance Framework	Establish roles, policies, and accountability for AI lifecycle management.
AI Threat Modeling	Identify and mitigate LLM-specific attack vectors like prompt injection and tool chaining.
AI Risk & Control Assessment	Benchmark governance, data, and oversight maturity using ISO 42001 & NIST AI RMF.
AI Detection & Monitoring	Enhance visibility with anomaly detection for AI behaviors and misuse.
AI Red-Team Simulation	Simulate attacks to expose weaknesses in LLM/agentic architectures.
Continuous Assurance	Quarterly reviews and governance updates aligned to evolving risks.

Key Benefits

• Strengthen AI governance aligned with ISO 42001 & NIST AI RMF
• Proactively identify and mitigate AI-specific risks
• Validate resilience with AI red-teaming
• Integrate continuous oversight into enterprise governance
• Build customer and regulator trust in AI adoption

Contact

DISC InfoSec | vCISO AI Governance Practice
Email: info@deurainfosec.com | Web: www.deurainfosec.com