

Summit AI Governance

AI Governance & Compliance • Risk, Privacy, and Operational Guardrails for GenAI

We help agencies and regulated enterprises deploy GenAI safely—by turning policy and standards into practical, auditable controls and artifacts (DPIA/PIA, ROPA, control mapping, evidence packs).

The problem

GenAI & agentic workflows are moving faster than governance and compliance.

What agencies face

- Rapid adoption of GenAI/agents across teams (inconsistent controls)
- Privacy, security, and records risks without standardized artifacts
- Procurement pressure: prove “safe to operate” to primes and auditors

What “good” looks like

- Repeatable guardrails + evidence (policies, registers, reviews)
- A clear risk framework for AI (governance, mapping, monitoring)
- Controls aligned to federal guidance and authorization paths

Standards we align to (examples)

- OMB M-24-10: governance and risk management expectations for agency use of AI
- NIST AI RMF 1.0: risk management functions + profile approach
- FedRAMP: cloud authorization approach aligned to NIST 800-53 controls

Our solution

A fast, practical path from “policy” → “operational controls” → “audit-ready evidence.”

1) Assess & triage

- Use-case inventory
- Risk triage (safety/rights)
- Data + system boundaries

2) Design guardrails

- Governance model + RACI
- DPIA/PIA + ROPA
- Control mapping + templates

3) Operationalize

- Review cadence + gates
- Evidence packs
- Training + playbooks

Result: a repeatable governance package you can reuse across programs—aligned to agency expectations and procurement review.

Artifacts we generate

Concrete deliverables that make compliance and reviews faster.

Privacy artifacts

- DPIA / PIA (risk, mitigations, residual risk)
- ROPA (records of processing activities)
- Data flow diagrams + retention/records notes
- Model/system impact & rights considerations

Governance artifacts

- AI policy & standards + review gates
- Use-case register + risk scoring + decisions
- Control mapping (e.g., NIST 800-53 / FedRAMP) and evidence packs
- Templates: model cards, prompt logs, testing checklists

Why this matters for procurement

Buyers and primes don't just want "we comply." They want artifacts that prove governance is real and repeatable—so delivery can scale beyond one-off reviews.

Standards alignment (at-a-glance)

How our artifacts map to common federal expectations.

Guidance / Standard	What it expects	Artifacts we deliver
OMB M-24-10	Agency governance & risk mgmt for AI (roles, oversight, controls)	Governance model, RACI, review gates, evidence packs
NIST AI RMF 1.0	Risk functions + profiles (GOV/MAP/MEASURE/MANAGE)	AI risk register, use-case triage, metrics, reporting cadence
FedRAMP + NIST 800-53	Security & privacy controls for cloud systems	Control mappings, SSP-ready evidence, implementation checklists

Training & enablement

Hands-on training to operationalize safe GenAI workflows in regulated environments.

Course modules (example)

- Agentic AI frameworks: orchestration, tools, memory patterns
- Prompt & context engineering: RAG fundamentals and eval basics
- Secure-by-design “AI-assisted dev” patterns + review checklists
- Governance in practice: approvals, documentation, evidence

Outcomes

- Teams use GenAI with consistent guardrails
- Reduced rework via standardized artifacts
- Clear roles, approvals, and audit trails
- Materials + templates to reuse post-training

Format (typical)

- 1–2 day hands-on workshop + lab exercises
- Pre-read + baseline questionnaire
- Post-training survey + completion certificates (optional)

Why Summit AI Governance

High-trust posture for government, primes, and regulated enterprises.

Key differentiators

- Veteran-led SDVOSB focused on AI governance + privacy + compliance
- Former Senior Director of AI Risk & Ethics at Lenovo
- Practical templates (not just advice): policies, registers, evidence
- Controls alignment for procurement and prime contractor review
- Fast “starter kit” approach to accelerate readiness in 30 days

Procurement identifiers (example)

UEI: S11FDVXMKQW1

CAGE: 146V9

NAICS: 541611, 541512, 611430, 541519

Location: Buffalo, NY

Engagement models

- Prime subcontractor (compliance / governance workstream)
- Micro-purchase / task order packages
- Training delivery (virtual or in-person)

Next step

Let's align on the use case, boundary, and approval path—then move fast.

Contact

Matthew Royal
COO, Summit AI Governance (SDVOSB)
Email: upstate.shipment@gmail.com
Phone: (716) 870-7241
Website: summitaigovernance.com

Suggested 20-minute kickoff agenda

- Target users + mission outcome
- Data boundary + system context
- Compliance path (OMB/NIST/FedRAMP context)
- Success metrics + timeline
- Next deliverable: starter artifact pack

We're ready to support pilots, scaling, or training delivery in regulated environments.