

2025 Daniel P. Madden
License: CC BY-SA 4.0

AI OSI Stack Governance Risk Map
Author: Daniel P. Madden
Version: v4 Blueprint Integration
Date: November 2025

> ## Normative Language Notice
> This document uses normative language consistent with ISO/IEC 42010 and NIST conventions.
> SHALL denotes mandatory requirements, SHOULD denotes strong recommendations, and MAY denotes optional practices.
> Interpretations SHALL preserve authorial intent: layered accountability, epistemic integrity, and human dignity as binding design constraints.

1. Layer-to-Governance Control Matrix

AI OSI Layer	Primary Governance Risks	Example Controls	Evidence Artifacts
--- --- --- ---			
L1 Physical Substrate	Hardware tampering, supply chain opacity, resilience failure Certified facility audits, redundant energy and cooling governance, tamper-evident custody GDS, DRR		
L2 Data Stewardship	Consent erosion, provenance drift, epistemic contamination Consent traceability ledgers, dataset review boards, epistemic hygiene playbooks ITP, DRR		
L3 Model Development	Bias amplification, evaluation blind spots, red-team blind coverage Composite evaluation harnesses, adversarial benchmarking cadences, persona-aligned regression suites OAM, GDS		
L4 Instruction & Control	Prompt injection, persona drift, affect misalignment Persona mandate enforcement, refusal logic penetration testing, affect boundary audits ITP, DRR, GDS		
L5 Reasoning Exchange	Ledger desynchronization, packet replay, counter-signature gaps AEIP handshake validation, deterministic replay checkpoints, cross-node quorum review ILE, OAM		
L6 Deployment & Integration	Runtime drift, change conflicts, incident opacity Change gating with governance approvals, blue/green stewardship protocols, incident rehearsal TRR, OAM		
L7 Governance Publication	Delayed disclosure, accountability gaps, civic legitimacy erosion Public disclosure cadence, multi-stakeholder review councils, archival notarization GDS, ILE		

2. Stewardship Notes

Governance councils SHALL maintain the above matrix as a living register. Controls MAY be tailored to sectoral mandates provided equivalent rigor, transparency, and dignity-first obligations are preserved. Artifact classes SHALL remain immutable to ensure cross-layer auditability.