DAGS

DEPLOYMENT AI GOVERNANCE STANDARD

DAGS v1.0 Normative Standard

D2 — Model and Vendor Visibility

Domain Overview

1. Purpose

This domain defines the mandatory visibility requirements for models, components, configuration states, and vendors that materially influence the behavior of a deployed AI system.

Its purpose is to ensure that, once an AI system is operational:

- The organization can identify what models and components are in use
- Exact model versions and configuration states are identifiable and attributable
- The origin, role, and update authority of third-party vendors are visible and documented
- Material dependencies affecting system behavior are known, bounded, and governable
- No deployed system operates with opaque, undocumented, or version-ambiguous behavioral sources

This domain is normative.

---

2. Visibility Objective

The objective of the Model and Vendor Visibility domain is to ensure that deployed AI systems are not black boxes at the governance layer.

Version: v1.0
Status: Published

Visibility under DAGS means the organization can:

- Identify the models and services that influence system behavior
- Identify the exact version of those models active at any given time
- Distinguish between internally controlled components and externally supplied components
- Determine where authority, responsibility, and risk reside
- Trace historical model versions and associated approvals when system behavior changes

Visibility is a prerequisite for accountability, traceability, and change governance.

---

3. Scope of Visibility

Visibility under this domain applies to all components that materially affect deployed behavior, including:

- Primary and secondary models
- Third-party APIs or AI services
- Embedded or integrated vendor components
- Update channels or externally controlled behavior modifiers
- Configuration parameters that materially influence system outputs

Visibility is required regardless of whether components are proprietary, licensed, internally developed, or externally hosted.

Version-level identification and retention are required for all models materially influencing system behavior.

---

4. Vendor Relationship Principle

Use of vendors does not reduce governance responsibility.

This domain requires that:

- Vendor involvement is explicitly identified
- Vendor roles and influence are documented
- Vendor update authority and change mechanisms are known
- Reliance on vendor opacity is not accepted as a governance condition

Organizations remain accountable for systems they deploy, irrespective of sourcing.

Vendor-provided documentation does not substitute for internal visibility obligations defined under this standard.

---

5. Relationship to Other Domains

Model and Vendor Visibility supports and enables:

- Governance and accountability (D1) by clarifying responsibility and approval boundaries
- Security and controls (D3) by enabling version traceability, configuration-state binding, and change authorization integrity
- Operational integration (D5) by enabling reconstruction capability and incident response grounded in version-aware evidence

Without version-level visibility and historical retention, change governance, output traceability, and decision reconstruction controls cannot function effectively.

This domain establishes the informational substrate required for cross-domain evidentiary integrity.

6. Boundary Conditions

This domain governs identification, attribution, and retention of model and vendor information, not:

- Evaluation of model quality or performance
- Assessment of vendor maturity or trustworthiness
- Contract negotiation strategy
- Technical inspection of model internals

Those concerns are outside scope unless they affect deployment-layer visibility, version determinism, or attribution.

7. Interpretive Notes

This overview provides context for the controls defined in D2_Requirements.

It does not introduce requirements, assessment logic, or examples.

Interpretation shall be governed by the normative requirements that follow.

8. Status

This Domain Overview is normative.

It is binding for DAGS v1.0 and all derivative artifacts unless explicitly superseded.

9. License & Authority

The Deployment AI Governance Standard (DAGS) is a publicly available governance standard made available for reference and implementation.

All intellectual property rights in DAGS, including the standard text, structure, methodology, and interpretive guidance, are retained by the DAGS Governing Body.

Public availability of this document does not grant any license or right to use DAGS for commercial, advisory, certification, assurance, or assessment purposes. Such uses may require separate authorization or licensing from the DAGS Governing Body.

No rights are granted by implication, estoppel, or public distribution.

Editorial, interpretive, versioning, and equivalency authority is retained exclusively by the DAGS Governing Body. No third party may issue authoritative interpretations, certifications, or compliance determinations without explicit written authorization.

Deployment AI Governance Standard (DAGS) v1.0
Status: Published