



DAGS v1.0 Normative Standard

D1 — Governance and Accountability

Normative Requirements

1. Purpose

This document defines the mandatory governance and accountability requirements for deployed AI systems under Domain D1 of the Deployment AI Governance Standard (DAGS) v1.0.

This domain establishes who is authorized to govern, how accountability is assigned, and how governance authority persists across operational change.

All requirements in this document are normative and binding.

2. Governance Ownership

D1.1 System Ownership

Each deployed AI system shall have a clearly designated system owner.

The system owner shall be accountable for:

- The system’s operational behavior
- Compliance with applicable governance requirements
- Oversight of post-deployment changes
- Maintenance of declared deployment scope



Ownership shall be formally documented and attributable.

D1.2 Authority to Govern

The system owner shall possess or be delegated explicit authority to govern the deployed AI system.

Authority shall include the ability to:

- Approve or reject changes meeting the definition of materially affecting behavior
- Enforce governance controls
- Escalate issues when governance requirements are not met
- Suspend or constrain system operation when required

Authority shall not be implied, symbolic, or informal.

D1.3 Governance Competence

Roles assigned governance authority or accountability shall demonstrate documented competence appropriate to the system’s risk classification.

Competence may include:

- Formal training
- Relevant certification
- Demonstrated governance experience
- Documented domain expertise

Competence shall be maintained across personnel transitions and shall not be presumed based solely on title or organizational position.



Governance authority without demonstrable competence is prohibited.

3. Accountability Assignment

D1.4 Accountability for Outcomes

Accountability for system outcomes shall be explicitly assigned.

The accountable role or function shall be identifiable and documented, regardless of:

- Vendor involvement
- Level of automation
- Use of third-party components

Accountability shall not be diffused, ambiguous, or shared without defined responsibility boundaries.

D1.5 Persistence of Accountability

Accountability shall persist across:

- System updates
- Configuration changes
- Vendor transitions
- Organizational restructuring

Changes in personnel, vendors, or structure shall not result in unassigned accountability.

Governance continuity shall be preserved during transitions.

4. Governance Structure

D1.6 Documented Governance Structure

Each deployed AI system shall operate within a documented governance structure.

The governance structure shall define:

- Decision-making authority
- Escalation paths
- Oversight responsibilities
- Change approval thresholds
- Materiality determination authority

Documentation shall be maintained, attributable, and accessible to relevant stakeholders.

D1.7 Separation of Duties

Where governance responsibilities are distributed, roles and responsibilities shall be clearly delineated.

Conflicting authorities shall not exist without documented resolution mechanisms.

Oversight roles shall not be structurally subordinate to routine operational control functions without explicit governance justification.

5. Oversight and Escalation

D1.8 Oversight Mechanism

An oversight mechanism shall exist to monitor system operation and governance adherence.

Oversight shall:

- Be assigned to identifiable authority
- Be capable of detecting governance-relevant issues
- Include independent review authority separate from routine operational monitoring
- Be empowered to initiate corrective action

Oversight mechanisms shall not be purely observational.

D1.9 Escalation Path

A defined escalation path shall exist for governance failures, anomalies, disputes, or constraint violations.

Escalation authority shall be:

- Documented
- Actionable
- Independent of routine system operation

Escalation processes shall not rely on informal practice.

6. Vendor and Third-Party Accountability

D1.10 Retained Accountability

Use of third-party models, services, integrations, or vendors shall not transfer governance accountability away from the deploying organization.

The deploying organization remains accountable for governance of the deployed system, including components meeting the definition of materially affecting behavior.

D1.11 Contractual Alignment

Where third parties are involved, contractual arrangements shall support governance accountability.

Contracts shall enable:

- Authority to review and constrain behavior
- Access to necessary governance-relevant information
- Ability to respond to changes meeting the definition of materially affecting behavior

Contractual gaps that prevent governance enforcement are prohibited.

7. Materiality Determination Governance

D1.12 Materiality Determination Authority

The authority responsible for determining whether a change or component meets the definition of materially affecting behavior shall be documented.



Materiality determinations shall:

- Be recorded
- Reference declared system scope
- Reference operational context
- Be subject to periodic reassessment

Materiality classification shall not be implicit or assumed.

8. Deployment Authorization and Scope

D1.13 Formal Deployment Authorization

A deployed AI system shall not enter production operation without documented, attributable authorization by the designated governing authority.

Authorization shall:

- Reference the declared deployment scope
- Reference active model version(s)
- Reference applicable operational constraints
- Be retained as a governance artifact

Unauthorized deployment is prohibited.

D1.14 Deployment Scope Declaration

Each deployed AI system shall maintain a formally documented deployment scope that explicitly defines:

- Intended use
- Prohibited use
- Authorized user classes
- Decision classes influenced in a manner meeting the definition of materially affecting behavior
- Data domains processed

Operation outside declared scope is prohibited absent formal reauthorization.

9. Prohibited Conditions

D1.15 Unowned Systems Prohibited

A deployed AI system shall not operate without:

- An assigned owner
 - Documented governance authority
 - Defined accountability
 - Demonstrated governance competence
-

D1.16 Implicit Governance Prohibited

Reliance on informal practice, institutional knowledge, undocumented authority, or assumed competence shall not be considered governance.



10. Applicability

All requirements in this document apply to all deployed AI systems within DAGS scope unless explicitly stated otherwise.

11. Status

This Requirements document is normative.

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

12. 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
Copyright © DAGS Governing Body
All Rights Reserved