



DAGS v1.0 Normative Standard

D5 — Operational Integration

Domain Overview

1. Purpose

This domain defines the mandatory operational integration requirements that ensure a deployed AI system is effectively embedded within organizational operations and governance processes.

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

- Governance controls are integrated into day-to-day operations
- Operational processes support accountable, controlled, and reconstructable system behavior
- AI systems are not isolated from standard operational oversight, and operational monitoring mechanisms support but do not substitute for independent governance review authority defined under D1.
- Governance remains effective throughout the system lifecycle
- Incidents and contested outcomes can be investigated using durable, version-aware evidence

This domain is normative.

© DAGS Governing Body. DAGS™ is a publicly available standard. Editorial and interpretive authority is retained exclusively by the DAGS Governing Body. Reference to or implementation of this standard does not imply certification, compliance, endorsement, or authorization unless expressly granted in writing by the DAGS Governing Body.	Version: v1.0 Status: Published
	Page 1 of 5



2. Operational Integration Objective

The objective of the Operational Integration domain is to ensure that AI governance functions in practice, not only in documentation.

Under DAGS, operational integration requires that:

- Governance controls are embedded into operational workflows
- Operational roles responsible for governance responsibilities demonstrate documented competence appropriate to system risk classification and can execute governance responsibilities
- AI systems are managed as part of normal operations, not as exceptions
- Incident handling processes are capable of interfacing with governance-relevant logs and configuration-state records
- Where incidents implicate vendor-controlled components, defined notification pathways exist

Operational integration shall include the ability to evaluate and respond to changes meeting the definition of materially affecting behavior in alignment with governance authority defined under D1 and change controls defined under D3.

Integration is necessary for governance to function in sustained and defensible ways.

3. Scope of the Domain

This domain applies to operational processes that meet the definition of materially affecting the governance of deployed AI systems, including:

- Integration of AI governance into operational procedures
- Alignment with incident management and response processes
- Operational readiness to manage system changes or failures



- Ongoing operation, maintenance, and oversight
- Reconstruction capability for contested decisions

Operational integration includes the ability to access and utilize artifacts generated under:

- Model and vendor visibility controls (D2)
- Security and traceability controls (D3)

The domain does not govern general business operations unrelated to AI system governance.

4. Relationship to Other Domains

Operational Integration connects and enables:

- Governance and accountability (D1) through operational execution and documented authorization use
- Model and vendor visibility (D2) by relying on version-level identification and historical retention
- Security and controls (D3) by operationalizing governance-relevant logging and configuration-state binding
- Ethics and responsible use (D4) by embedding enforcement, oversight, and intervention mechanisms into daily operations

Without operational integration, governance requirements cannot be sustained, evidenced, or defended under scrutiny.

This domain ensures that governance artifacts created under other domains are usable within real-world operational and incident contexts.

5. Boundary Conditions

This domain governs how governance operates within organizational processes, not:

- Business strategy or planning
- Workforce training unrelated to governance responsibilities
- Tool selection or operational optimization
- Model design or training-stage practices

Such concerns are outside scope unless they meet the definition of materially affecting governance execution, reconstruction capability, or incident response.

6. Interpretive Notes

This overview provides context for the controls defined in D5_Requirements.

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

Interpretation shall be governed by the normative requirements that follow.

7. Status

This Domain Overview is normative.

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



8. 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

© DAGS Governing Body. DAGS™ is a publicly available standard. Editorial and interpretive authority is retained exclusively by the DAGS Governing Body. Reference to or implementation of this standard does not imply certification, compliance, endorsement, or authorization unless expressly granted in writing by the DAGS Governing Body.	Version: v1.0 Status: Published
	Page 5 of 5