

# The Precedent Sufficiency Doctrine

## Establishing Legitimacy Thresholds for AI in Governance

WHITE PAPER

Kathryn G. Varnes  
Founder, Athosphere LLC  
MLS-LP (Administrative Law)  
Authoritative, Integrated Edition (v19)

January 2026

### Status and Use

This white paper articulates a governance doctrine intended to inform policy, institutional decision-making, and scholarly discussion. It does not constitute legal advice, regulatory guidance, or a representation of compliance with any law or standard. Adoption or application of the doctrine is voluntary and remains subject to applicable legal, regulatory, and organizational authority.

© 2026 Athosphere LLC. All rights reserved.

## Abstract

Artificial intelligence is increasingly deployed as a default solution in governance, regulation, and organizational decision-making. Most contemporary AI governance frameworks assume that deployment is appropriate and focus instead on managing downstream risk, performance, or compliance. This paper challenges that assumption. The Precedent Sufficiency Doctrine establishes a legitimacy-first standard for AI governance. It treats AI not as an incremental upgrade, but as a deviation from established human governance that must be affirmatively justified before use. Under the doctrine, AI may be introduced only where existing non-AI governance mechanisms are demonstrably insufficient and where the deploying authority retains sovereign control across the system's full lifecycle.

The doctrine operates prior to technical or risk-based frameworks such as the NIST AI Risk Management Framework or the EU Artificial Intelligence Act. It assigns burdens of justification to proponents of AI use, identifies non-delegable human functions, and defines binding thresholds for legitimacy, sovereignty, and control. It is intended for policymakers, regulators, boards, and governance leaders seeking to determine not how to optimize AI systems, but whether they should be used at all.

## Introduction

Artificial intelligence has rapidly moved from experimental tool to embedded decision infrastructure. Across public administration, healthcare, finance, and enterprise operations, AI systems increasingly influence—or effectively determine—outcomes that were historically governed by human institutions.

Most contemporary AI governance efforts focus on managing risk after deployment: accuracy, bias, robustness, transparency, or post-market monitoring. While important, these approaches generally presume that AI deployment is appropriate or inevitable. They rarely address a more foundational question: when is it legitimate to delegate governance functions to artificial intelligence at all?

The Precedent Sufficiency Doctrine is designed to answer that question. Drawing on principles of administrative law, institutional legitimacy, and non-delegation, it treats AI deployment as a deviation from established governance precedent rather than a neutral technological upgrade. Under this doctrine, the burden rests with the proponent of AI to demonstrate both necessity and governability, including sustained sovereign control. This doctrine is intentionally conservative. It prioritizes accountability, sovereignty, and human institutional integrity over efficiency, scale, or innovation pressure. The sections that follow reproduce the doctrine in full. The doctrine is normative and binding in structure; explanatory material is provided solely to aid interpretation and does not alter its operative force.

*Artificial intelligence is not a default solution; it is a deviation from established governance and must justify both its necessity and its sovereign legitimacy before it is permitted.*

---

# The Precedent Sufficiency Doctrine

## PART I—FOUNDATIONAL PREMISE AND SCOPE

### I. Statement of Doctrine

Artificial intelligence shall not be introduced into any decision-making context unless existing governance mechanisms are demonstrated to be insufficient to address the problem at hand.

AI deployment constitutes a deviation from established governance precedent and therefore requires affirmative justification prior to design, procurement, development, training, deployment, renewal, retraining, upgrade, replacement, or continued operation. This doctrine applies with heightened scrutiny where AI influences consequential decisions—those that materially affect an individual's rights, safety, liberty, dignity, privacy, access to services, legal status, or protected interests under applicable law. AI shall further not be introduced where the deploying authority lacks sovereign control over the AI system's design, operation, security, lifecycle management, or continued availability.

Governance legitimacy requires not only necessity, but the capacity to govern. Dependency on external sovereigns, foreign corporations, non-subordinate technical infrastructure, opaque vendor control, or unmodifiable models constitutes a threshold governance defect.

## **II. Presumptions**

### **II.a. Governance Sufficiency Presumption**

Existing non-AI governance controls are presumed sufficient unless proven otherwise. This presumption applies regardless of technological feasibility, market availability, competitive or financial pressure, anticipated efficiency gains, vendor recommendations, or prevailing industry adoption.

Efficiency, popularity, or innovation pressure alone do not rebut the presumption.

### **II.b. Sovereign Sufficiency Presumption**

AI systems over which the deploying authority lacks independent operational and lifecycle control are presumed governance-insufficient, regardless of accuracy, certification, contractual assurances, or industry endorsement.

Absent sovereign control and AI deployment is presumptively illegitimate.

Sovereign control includes protection against silent retraining, unapproved model updates, dependency changes, or other lifecycle modifications beyond the deploying authority's independent control.

## **III. Scope of Application (Mode-Neutrality)**

This doctrine applies irrespective of the manner in which AI is introduced, including standalone tools, embedded systems, third-party vendors, APIs, cloud services, software-as-a-service, upgrades, or indirect functionality.

Undisclosed or indirect introduction of AI ("shadow AI") constitutes a governance failure.

## **IV. Temporal Application**

This doctrine applies to all AI deployments initiated after adoption; material modifications to existing systems; expansion to new decision contexts, populations, or uses; and renewal, retraining, replacement, or upgrade introducing or altering AI functionality.

AI systems deployed prior to adoption may operate during a defined conformance review period but shall not be expanded absent a determination under this doctrine.

Loss of sovereign control, dependency changes, export controls, sanctions, or vendor withdrawal trigger immediate re-evaluation.

## **V. Definition of Artificial Intelligence**

Artificial intelligence means any system whose decision logic cannot be fully specified in advance and whose outputs are generated through learning from data, adaptive modeling, or probabilistic inference rather than fixed, deterministic logic.

When classification is uncertain, the functional test applies: if the system's logic cannot be fully specified in advance and changes based on data, it is AI for purposes of this doctrine.

## PART II — JUSTIFICATION AND LIMITS ON DELEGATION

### VI. Burden of Justification

The proponent of AI deployment bears the burden of demonstrating that:

1. The problem is clearly defined and documented.
2. Existing governance precedent exists.
3. Existing controls are insufficient due to scale, speed, volume, complexity, or human safety limitations.
4. The insufficiency cannot reasonably be resolved through process redesign, policy enforcement, training, human resourcing, deterministic automation, or conventional software.
5. The AI system can be independently governed across its full lifecycle, including updates, retraining, suspension, withdrawal, kill-switch authority, and continuity under stress or vendor failure.

Manufactured insufficiency—intentional degradation or under-resourcing of non-AI governance to justify AI deployment—invalidates justification.

### VII. Non-Delegable Elements

The following functions are non-delegable: moral judgment, legal accountability, due process determinations, discretion affecting dignity, liberty, life, or privacy, and authority to impose irreversible harm.

AI may support but shall not replace these functions.

Human oversight must be substantive, informed, and capable of independent exercise. Rubber-stamp review does not satisfy this requirement.

### VIII. Information Integrity and Human Harm

Informational harm—including manipulation, distortion, covert influence, fabricated authority, or degraded truthfulness—constitutes human harm.

Human risk, including automation bias, authority displacement, skill atrophy, moral injury, and accountability dilution, is an independent governance harm.

Informational harm or human risk may independently bar AI deployment regardless of technical performance or governance structure.

## PART III — GOVERNANCE AUTHORITY AND DECISION STRUCTURE

### IX. Governance Authority and Charter Requirement

Where AI deployment is permitted, governance authority shall be exercised through a formally chartered governance body with documented authority, roles, and decision rights. Governance charters shall define scope of authority, decision power, accountability and escalation paths, membership composition, and documentation obligations.

Governance structure does not legitimize otherwise impermissible delegation.

## **X. Precedent Analysis Requirement**

Prior to deployment, a documented Precedent Analysis shall determine how the problem has historically been governed, which controls remain effective, which fail to scale, whether AI augments or supplants precedent, and whether AI displaces sovereign governance authority.

## **XI. Product Classification Requirement**

AI systems shall be classified based on authority exercised, not technical complexity:

- Informational
- Advisory
- Determinative
- Autonomous (High-Risk)
- Sovereign-Equivalent

Ambiguity escalates classification upward. Highest-risk use governs.

## **XII. Governance Maturity and Control Mapping**

Governance rigor shall scale with product classification, duration of deployment, data volume and sensitivity, regulatory exposure, and human and informational risk.

Higher categories require formal gate reviews, kill-switch testing, independent oversight, reauthorization cadence, and license-like approvals where appropriate.

# **PART IV — TRUST, DETERMINATIONS, AND LIFECYCLE CONTROL**

## **XIII. Information Trust Rating (Binding)**

AI systems shall be assigned an Information Trust Rating: Verified, Conditional, Degraded, or Insufficient.

Ratings are assigned by the governance authority, reassessed periodically, and automatically downgraded upon manipulation, provenance failure, or loss of control. Systems rated Degraded or Insufficient are prohibited from consequential use.

## **XIV. Determination Outcomes**

Application of the doctrine results in one of the following binding determinations:

- AI Not Warranted
- AI Augmentation Permitted
- AI Deployment Conditionally Permitted
- AI Deployment Prohibited

## **XV. Emergency, Incident, and Restoration Provisions**

Emergency variances may be granted only where an imminent threat to life or safety exists, duration is strictly limited, human authority remains dominant, and post-incident review is mandatory.

Where AI was justified due to insufficiency, periodic review shall determine whether restored governance permits withdrawal.

## **PART V — HIERARCHY, ANNEXES, AND STRESS CONDITIONS**

### **XVI. Relationship to Existing Standards**

This doctrine operates prior to and independent of frameworks and standards, including the NIST AI Risk Management Framework, the EU Artificial Intelligence Act, ISO/IEC 42001, and corporate AI ethics programs.

Such frameworks apply only after legitimacy and sovereign sufficiency are established.

### **XVII. Hierarchy of Authority (Anti-Dilution Clause)**

This doctrine governs legitimacy. Governance charters govern execution. Operational annexes govern control.

No governance structure, process, certification, audit, or tool may legitimize an otherwise impermissible delegation.

Operational annexes A–G are binding instruments incorporated by reference and apply during normal operation, stress, failure, misuse, and institutional decay. Absence of evidence under stress conditions shall be construed as absence of governance.

### **XVIII. Binding Operational Annexes (Incorporation by Reference)**

The following annexes are incorporated by reference and are binding by doctrine:

- A. Failure Modes
- B. Governance Persistence and Anti-Normalization
- C. Evidence Freshness
- D. Exit Viability and Continuity
- E. Human Reliance and Automation Bias
- F. Downstream Propagation
- G. Independent Challenge and Non-Delegation

No framework, audit, certification, or vendor assurance may substitute for compliance with these annexes.

### **XVIII-A. Doctrine Stress Conditions (Failure Anticipation Clause)**

The sufficiency of this doctrine shall be assessed not only under ordinary operation, but under foreseeable stress conditions, including post-incident scrutiny, temporal degradation, delegation pressure, human over-reliance, and continuity failure.

Governance mechanisms must withstand misuse, neglect, degradation, and adverse incentives. Failure to anticipate and govern these conditions constitutes a governance defect independent of model accuracy or compliance with external standards.

## PART VI — CANONICAL CLOSURE

### XIX. Canonical Doctrine Sentence

Artificial intelligence is not a default solution; it is a deviation from established governance and must justify both its necessity and its sovereign legitimacy before it is permitted.

### XX. Why This Is a Doctrine

It establishes presumptions.  
It assigns burdens of proof.  
It governs legitimacy, not optimization.  
It constrains authority, not behavior.  
It binds decisions, not aspirations.  
That is doctrine.

## Conclusion

As artificial intelligence becomes embedded in decision-making systems, the risk is no longer merely technical failure, but institutional erosion. The Precedent Sufficiency Doctrine offers a governance standard that restores legitimacy as the primary threshold for AI use.

By establishing presumptions against deployment, assigning burdens of proof, and enforcing sovereign control and non-delegation, the doctrine provides a durable foundation for responsible AI governance. It is designed to withstand time, pressure, vendor dependence, and institutional decay.

This white paper invites careful adoption, critique, and application across public and private governance contexts. Its purpose is not to accelerate AI deployment, but to ensure that where AI is used, it is used legitimately.

This white paper reproduces the Precedent Sufficiency Doctrine for AI Governance in full. No operative provisions have been removed, altered, or weakened for publication.

---

#### AI Acknowledgment

Assistance with language, structure, and organization was provided using ChatGPT (OpenAI, 2025). All legal reasoning, factual analysis, and conclusions are my own.