theIOM.org

The Infrastructure Operating Model

IOM Standard — Version 1.0

A vendor-neutral specification for the infrastructure authority layer

Field	Value
Status	Proposed open standard — v1.0, draft for public comment
Approach	Practitioner-led · vendor-neutral · openly governed
Steward	The theIOM.org working group
License	Creative Commons Attribution 4.0 (CC BY 4.0)
Feedback	working-group@theiom.org

This is a draft published for open review. It is not a frozen specification.

Contents

Abstract

As infrastructure becomes software-defined, distributed, and increasingly autonomous, organizations face a structural gap between execution and authority: infrastructure can now act faster than any human or tool can decide what should be allowed. Existing tools optimize configuration, automation, and observability, but none provides a shared, authoritative model of what infrastructure *exists*, what it is *intended* to do, and what actions are *legitimate*.

This document defines the Infrastructure Operating Model (IOM): the authoritative layer that governs infrastructure understanding, intent, ownership, and constraints, and that validates actions against them before execution occurs. The IOM is a vendor-neutral operating model — not a product — on which automation, control planes, and infrastructure AI can operate safely, explainably, and at scale.

Status of This Document

INFORMATIVE

This is a proposed open standard, published as v1.0 for public comment. It is practitioner-led and stewarded by the theIOM.org working group. It is not a frozen or final specification; it is intended to evolve through open review. Changes are adopted through open review and issued as new, versioned releases with an accompanying change note.

This document contains **normative** sections, which define mandatory requirements, and **informative** sections, which provide context and guidance. The key words **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** are to be interpreted as described in RFC 2119.

Feedback, conformance questions, and proposed changes are welcome at **working-group@theiom.org**.

1. Scope

NORMATIVE

This standard defines:

- The concept of an Infrastructure Operating Model (IOM) and its canonical definition
- The minimum functional and structural requirements an IOM MUST satisfy
- The role of the IOM in governing infrastructure, automation, control planes, and infrastructure AI
- The criteria by which an implementation may claim conformance

This standard does not specify vendor products, implementation architectures, or tooling choices.

An IOM is distinct from — and this standard does not define — the following. An IOM **governs** these capabilities; it does not replace them:

- **Automation or orchestration.** An IOM decides what is legitimate; it does not execute changes.

- **Configuration management (CMDB) or asset inventory.** An IOM is a continuously reconciled, authoritative model — not a static record.
- **Infrastructure as code (IaC).** IaC expresses desired configuration; an IOM governs whether a change is permitted before it is applied.
- **Identity and access management.** IAM authenticates actors; an IOM authorizes actions against intent.
- **Observability or monitoring.** Observability is runtime evidence, not authority.
- **A digital twin.** A digital twin is an advisory, simulation-oriented representation positioned outside the execution path; an IOM is authoritative and sits in the path of change.
- **A single product or vendor.** An IOM is an operating model and a standard, not a SKU.

2. The Authority Gap

INFORMATIVE

Modern infrastructure environments operate continuously, while governance mechanisms remain episodic, manual, or tool-specific. This mismatch creates systemic risk, delivery friction, and control failures that cannot be resolved through automation, observability, or policy engines alone.

As infrastructure becomes software-defined and increasingly autonomous, authority is too often inferred rather than explicitly modeled. The result is fragile automation, inconsistent enforcement, unsafe AI-driven decisions, and governance that arrives after impact rather than before it.

Infrastructure built for human decision speed cannot govern infrastructure operating at machine speed. Closing this authority gap is the purpose of an IOM.

3. Definition of an Infrastructure Operating Model

NORMATIVE

An Infrastructure Operating Model is the authoritative layer that defines what infrastructure exists, what it is intended to do, and what actions are legitimate — before execution occurs.

An IOM MUST:

- Operate continuously and independently of any single execution tool
- Maintain authoritative understanding of infrastructure state, intent, ownership, and constraints
- Coordinate human, automated, and AI-driven actors under a single, explicit authority
- Determine the legitimacy of a change before it executes, enforce constraints during execution, and produce evidence after

4. Core Principles

NORMATIVE

An IOM MUST embody the following principles.

1. **Continuous governance.** Governance MUST operate in real time, not through episodic review processes.
2. **System-level authority.** Authority MUST be explicit, durable, and independent of individual tools or workflows — a layer the rest of the operating model answers to.
3. **Intent-driven control.** Infrastructure behavior MUST be evaluated against explicit, declared intent — not inferred from signals.
4. **Governance before execution.** Legitimacy MUST be evaluated and enforced prior to execution, not only observed after failure.
5. **Integration, not replacement.** An IOM MUST integrate with and govern existing execution tools — control planes, pipelines, cloud, identity, and observability — rather than replace them.

5. The Canonical Infrastructure Model

NORMATIVE

An IOM MUST be anchored by a canonical infrastructure model: a continuously reconciled, authoritative representation of infrastructure as it exists, including:

- Current state of infrastructure elements across cloud, network, identity, and on-premises environments
- Structural relationships, dependencies, and trust boundaries
- Constraints, ownership, and environmental context

The canonical model MUST serve as authoritative context for governance decisions. It is distinct from a digital twin or an observability dashboard: it MUST NOT be advisory, simulation-oriented, or positioned outside the execution path, and it MUST NOT be treated as a mere visualization artifact. It is a living model, reconciled against reality — *not a snapshot.*

6. Blueprint-Derived Intent

NORMATIVE

An IOM MUST derive infrastructure intent from explicit blueprints that define how infrastructure is designed to exist and behave.

Blueprints MUST:

- Encode structural patterns, constraints, and allowed variations
- Be versioned and attributable to owners
- Exist independently of execution mechanisms
- Be reusable across environments and platforms

Intent MUST NOT be inferred solely from runtime behavior, configuration drift, or observability data.

7. Ownership and Decision Authority

NORMATIVE

An IOM MUST explicitly encode ownership of infrastructure elements, decision rights for change and exception handling, and escalation paths for conflict and risk.

Ownership and authority MUST be machine-readable, enforceable prior to execution, and distinguishable between human and system actors. When something changes or fails, ownership and blast radius MUST be deterministic — known in advance, not reconstructed under pressure.

8. Constraints and Boundaries

NORMATIVE

An IOM MUST explicitly define the constraints and boundaries within which infrastructure may operate — including, but not limited to, how data is permitted to move across services, environments, and trust boundaries.

Observed behavior and data flows MUST be continuously evaluated against these defined constraints and intent.

9. Observability as Evidence

NORMATIVE

Observability MUST be treated as runtime evidence, not as a governance mechanism. Observability systems MAY inform enforcement decisions, but MUST NOT be the source of authority or intent.

10. Governance in Motion

NORMATIVE

An IOM MUST govern infrastructure across the full lifecycle of a change:

- **Before execution —** authorization and legitimacy: is this action allowed, in this context, by this actor?
- **During execution —** constraint enforcement.
- **After execution —** verification, evidence, and learning that refines the model and intent.

Governance implemented solely through tickets, approvals, or post-hoc review does NOT satisfy this requirement.

11. Relationship to Zero Trust

NORMATIVE

An IOM complements and extends Zero Trust. Zero Trust authenticates and authorizes the actor at the point of access; an IOM evaluates the legitimacy of the action itself against authoritative intent. The two are layered, not alternatives.

To align with Zero Trust principles, an IOM MUST:

- Treat every infrastructure change as a trust decision evaluated against intent
- Support continuous least privilege
- Evaluate trust dynamically rather than statically

In short: Zero Trust governs *who* may act; the IOM governs *what* may be done.

12. Infrastructure AI Governance

NORMATIVE

Where infrastructure AI is present, an IOM MUST evaluate AI-proposed actions against authoritative intent, enforce constraints prior to execution, and ensure decisions are explainable and auditable.

AI systems MUST NOT operate outside the authority defined by the IOM. Because AI removes the human who previously supplied authority in the moment, the IOM becomes the layer that supplies it instead.

13. Expected Outcomes

INFORMATIVE

Organizations that govern infrastructure with an IOM typically move toward:

- Predictable, governed change rather than probabilistic, review-dependent change
- Risk prevented before impact rather than discovered after it
- Continuous audit readiness rather than retrospective evidence assembly
- Durable, trustworthy automation and AI adoption

14. Conformance

NORMATIVE

An implementation conforms to this standard if and only if it satisfies all MUST requirements herein, across the six capability dimensions of the IOM:

1. Infrastructure State Modeling
2. Intent and Blueprint Governance
3. Continuous Reconciliation
4. Ownership and Accountability
5. Governance at the Point of Execution
6. Evidence and Auditability

Partial implementations SHOULD NOT claim IOM conformance and MAY be described as IOM-informed. Any system that infers intent solely from observed behavior, runtime telemetry, or tool configuration does not conform to this standard.

15. Stewardship, Governance, and Feedback

INFORMATIVE

This standard is stewarded by the theIOM.org working group as a vendor-neutral, practitioner-led effort. It is published openly for public comment and is licensed under Creative Commons Attribution 4.0 (CC BY 4.0): it may be shared and adapted, including commercially, with attribution to theIOM.org.

Changes are adopted through open review and issued as versioned releases with a change note. Proposed changes, conformance questions, and requests to participate are welcome at **working-group@theiom.org**. This v1.0 draft supersedes no prior version.

16. Terminology and Definitions

NORMATIVE

Infrastructure Operating Model (IOM)
The authoritative layer that defines what infrastructure exists, what it is intended to do, and what actions are legitimate, before execution occurs.

Authority layer
The system-level layer that holds infrastructure intent and constraints and to which execution defers before acting.

Authority
The formally defined right to permit, deny, or constrain infrastructure behavior prior to execution.

Intent
Explicit, blueprint-derived declarations describing how infrastructure is designed to exist and behave.

Blueprint
A reusable, versioned specification that encodes structural patterns, constraints, and allowed variations, from which infrastructure intent is derived.

Canonical infrastructure model
A continuously reconciled, authoritative representation of infrastructure state, relationships, ownership, and constraints. Distinct from a digital twin: it is authoritative and in the execution path, not advisory or simulation-oriented.

Reconciliation
The continuous comparison of intended state, built state, and actual running state, enabling drift to be prevented rather than merely detected.

Legitimacy
The property of a proposed action being permitted, in context, by an accountable owner, within defined constraints.

Control plane
A system responsible for executing infrastructure changes. Control planes operate downstream of, and are governed by, the IOM.

Infrastructure AI

Any artificial intelligence system capable of proposing, executing, or influencing infrastructure-level decisions or actions.

Appendix A — Conformance Checklist

NORMATIVE

An implementation claiming conformance MUST satisfy every requirement below. Failure to meet any single requirement constitutes non-conformance.

✓	Capability dimension	Conformance requirement (all MUST be met)
☐	**Infrastructure State Modeling**	Maintains a continuously reconciled, authoritative infrastructure model spanning cloud, network, identity, and on-premises.
☐	**Intent & Blueprint Governance**	Derives intent from explicit, versioned, attributable blueprints — not from inferred runtime behavior.
☐	**Continuous Reconciliation**	Continuously reconciles intended, built, and running state to prevent drift before it becomes exposure.
☐	**Ownership & Accountability**	Encodes ownership, decision rights, and blast radius in machine-readable form; accountability is deterministic.
☐	**Governance at the Point of Execution**	Validates and enforces every change against intent before execution; ticket/approval-only governance does not qualify.
☐	**Evidence & Auditability**	Produces audit-ready evidence as a byproduct of operation; treats observability as evidence, not authority.
☐	**AI governance (where present)**	Evaluates AI-proposed actions against authoritative intent and enforces constraints before execution.

Appendix B — Mapping to the IOM Maturity Model

INFORMATIVE

Conformance with this standard is binary: an implementation either meets all requirements or it does not. The IOM Maturity Model, published in the IOM Starter Kit, provides the graduated self-assessment organizations use to locate themselves on the path toward conformance.

It scores an organization across the same six capability dimensions used in this standard. Each dimension is assessed against four sub-criteria on a 0–3 scale (None → Partial → Defined → Governed), for a maximum of 12 per dimension and 72 overall. Scores map to four maturity bands:

Maturity band	Characteristic
Pre-IOM (0–18)	Authority is implicit and tool-specific; governance is episodic and manual.
Emerging (19–36)	Capabilities exist in isolated pockets; inconsistent across teams and environments.
Developing (37–54)	Capabilities are documented, repeatable, and applied across most environments.

Maturity band	Characteristic
Governed (55–72)	Capabilities are continuously operating, machine-enforced, with improvement loops — the conformant end-state.

A “Governed” score indicates an organization has reached the operating posture this standard requires. The Starter Kit is available at **theIOM.org**.