AGCP Governance Capability Assessment Report

Governance-Scope-First Assessment

Acme Supply Company

AI Execution Governance Architecture

Assessment Date	2026-06-01
Assessment Type	Registry Assessment
Assessment Scope	AI-assisted semantic-equivalence registry assessment with source inspection and limited best-effort test execution of the synthetic Acme target package.
Repository Version	0.1.0
Registry Identifier	ACME-SUPPLY-AI-EGA-2026-REGISTRY-DEMO
Assessment Status	Complete - illustrative registry assessment
Assessor	AI-assisted assessor using Project Instructions v2.6

Contents

Assessment Metadata

Field	Value
Organization	Acme Supply Company
System / Project	AI Execution Governance Architecture
Assessment Date	2026-06-01
Assessment Type	Registry Assessment
Assessment Scope	AI-assisted semantic-equivalence registry assessment with source inspection and limited best-effort test execution of the synthetic Acme target package.
Repository Version	0.1.0
Registry Identifier	ACME-SUPPLY-AI-EGA-2026-REGISTRY-DEMO
Assessment Status	Complete - illustrative registry assessment
Assessor	AI-assisted assessor using Project Instructions v2.6
Methodology Version	Project Instructions v2.6
Template Identifier	report_template.tex.j2
Template Version	report_template.tex.j2 updated 2026-06-01
Renderer Identifier	render.py
Renderer Version	render.py project source, 2026-06-01
Test Suite Version	AGCP.ai Conformance Test Suite TC-001 through TC-093

Assessment Basis

Field	Value
Assessment Basis	• source_review • architecture_review • semantic_equivalency_analysis • evidence_inspection • limited_test_execution
Test Execution Scope	Limited best-effort execution of the target pytest suite; full TC-001 through TC-093 assured conformance suite was not executed.
Assessment Limitations	• Synthetic target package; not a production system assessment. • Registry Assessment findings are AI-assisted semantic-equivalence determinations, not Verified Assessment or Assured Assessment findings. • Full AGCP TC-001 through TC-093 test engineering, retained screenshots, environment capture, and version-controlled test evidence were not performed.

1 Executive Summary

AGCP is a requirements-based governance assessment and conformance framework. This assessment characterizes observed governance scope, demonstrated governance capabilities, semantic equivalency, and AGCP conformance. It does not assume that full AGCP conformance is the target owner's design objective.

1.1 Assessment Outcome

Category	Assessment
Governance Maturity	Moderate within proposal-time governance scope
Governance Scope Maturity	Clear proposal-time governance and evidence scope with intentional commit-bound omissions
Semantic Equivalency	Strong for proposal envelope, authorization artifact, and evidence concepts; limited for commit-bound admissibility and canonical state
Capability Verification Readiness	Registry-ready for selected evidence and auditability capabilities; further assessment required for most runtime governance claims
Conformance Readiness	Partial L1-L3 demonstration; L4 commit-bound execution semantics remain materially non-conformant; L5 largely not assessed
Overall Assessment	The target is a useful illustrative registry assessment example for distinguishing provenance-rich proposal-time authorization from AGCP commit-bound runtime governance.

1.2 Strengths

- Structured proposal envelopes with required fields are enforced.
- Provenance validation, proposal-time policy evaluation, authorization references, HITL quorum, and hash-linked ledger records are implemented.
- The package intentionally includes a stale-authorization test that exposes the core commit-bound governance gap.

1.3 Partial Capabilities

- Runtime governance is present as proposal-time mediation and token-gated commit, but not as commit-bound admissibility.
- Human authorization controls support quorum but not real cryptographic approval artifacts or timeout/cancellation lifecycle.
- Tenant isolation is tenant-scoped at submit and commit but not fully demonstrable across read, policy, approval, and ledger APIs.

1.4 Capabilities Not Demonstrated

- Commit-bound canonical-state re-evaluation.
- Ledger-derived lifecycle state as the sole authoritative state model.
- DEGRADED lifecycle semantics and re-evaluation before authorization retention or execution.

1.5 Capabilities Outside Observed Scope

- Multi-agent governance.
- Delegation governance.
- Cross-implementation interoperability and node-independent deterministic evaluation.

1.6 Potential Governance Expansion Areas

- Add commit-time canonical-state re-resolution and assumption rebinding.
- Replace simulated HITL signature flags with verifiable approval artifacts.
- Add DEGRADED lifecycle state and retained test evidence for stale assumptions.

2 Architecture Assessment

2.1 System Purpose

The target mediates AI-assisted procurement, inventory, and logistics action proposals before downstream execution systems are invoked.

2.2 Architecture Summary

The architecture combines schema-constrained proposal envelopes, tenant and actor context, provenance validation, proposal-time policy evaluation, human approval for selected actions, signed authorization references, token-gated execution, and hash-linked audit evidence. It intentionally omits commit bind-time re-evaluation against current canonical state.

2.3 Governance Boundaries

- Governed proposal submission and validation.
- Proposal-time policy and invariant evaluation.
- HITL approval for selected high-impact actions.
- Commit gateway authorization-token validation.
- Append-only audit event recording.

2.4 Governance Subjects

- Inventory adjustment proposals.
- Supplier onboarding proposals.
- Purchase-order approval proposals.
- Logistics rerouting proposals.
- AI-agent tool invocation proposals.

2.5 Governance Authorities

- GovernanceEngine policy logic.
- Tenant operational status records.
- HITL approvers represented by approver IDs.
- Authorization token service.
- Execution gateway commit path.

2.6 Governance Artifacts

- Proposal envelope.
- Provenance dictionary.
- Authorization token.
- ProposalRecord lifecycle status.
- Hash-linked ledger events.
- ExecutionReceipt and Refusal events.

2.7 Governance Architecture Classification

Classification	Assessment
Runtime Governance	Partial - proposal-time and token-gated runtime controls exist, but commit-bound admissibility is absent.
Workflow Governance	Partial - lifecycle states are mutable and minimal.
Risk Governance	Limited - simple policy thresholds drive HITL decisions.
Audit Governance	Strong for synthetic hash-linked events.
Policy Governance	Partial - policy is hard-coded rather than externalized.
Authorization Governance	Partial - authorization artifacts exist but are not fully commit-bound.
Hybrid Governance	Moderate - combines policy checks, HITL, provenance, and execution token gating.

3 Governance Scope Analysis

This section describes the governance problem the system appears designed to solve. Scope interpretation provides context for capability and conformance findings but does not alter AGCP conformance results.

3.1 Declared Objective

Illustrate buyer-selectable AI execution governance features using a synthetic Acme Supply Company architecture.

3.2 Observed Objective

Demonstrate provenance-rich proposal-time governance and token-gated execution while intentionally exposing the absence of commit-bound canonical-state re-evaluation.

3.3 Primary Focus Areas

- Proposal envelope governance.
- Substrate provenance validation.
- Proposal-time policy and invariant evaluation.

- Authorization token issuance and validation.
- Governance evidence recording.

3.4 Secondary Focus Areas

- HITL quorum for selected actions.
- Tenant scoping.
- Idempotent replay for identical proposal payloads.

3.5 Deferred Capabilities

- Commit-bound canonical-state re-evaluation.
- Ledger-derived lifecycle state.
- DEGRADED state handling.
- Real cryptographic HITL approval artifacts.

3.6 Capabilities Outside Observed Scope

- Multi-agent coordination.
- Delegated governance chains.
- Cross-implementation interoperability.
- Multi-node deterministic evaluation.

3.7 Scope Assessment

The observed scope is intentionally narrower than full AGCP conformance. The target is best understood as a proposal-time governance and authorization-gateway example rather than a complete AGCP control plane.

3.8 Scope Alignment Summary

Findings should be interpreted as a registry-style characterization of demonstrated governance features and gaps, not as a claim that the system was designed to satisfy every AGCP requirement.

4 Governance Capability Assessment

Capability assessment characterizes demonstrated governance capabilities independently from AGCP conformance. The scope classification indicates whether each capability appears central, supporting, deferred, outside observed scope, or unknown.

4.1 Capability Matrix

Capability Area	Status	Scope Classification	Confidence
Runtime Governance	Partial	Core Scope	High
Governance Evidence	Verified	Core Scope	High
Human Authorization Controls	Partial	Supporting Scope	Medium
Deterministic Governance	Partial	Supporting Scope	Medium
Governance Continuity	Partial	Supporting Scope	Medium
Governance Degradation Management	Partial	Deferred	High
Multi-Agent Governance	Not Present	Outside Observed Scope	High
Delegation Governance	Not Present	Outside Observed Scope	High
Tenant Isolation	Partial	Supporting Scope	Medium
Governance Auditability	Verified	Core Scope	High

4.2 Capability Findings

4.2.1 Runtime Governance

Field	Finding
Status / Assessment	Partial
Scope Classification	Core Scope
Confidence	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The target mediates proposed actions at runtime through a GovernanceEngine that validates envelopes, tenant state, provenance, policy applicability, and proposal-time invariants before issuing authorization or refusal outcomes. Execution is also mediated by an authorization-token commit gateway. This is a meaningful runtime governance pattern, but it is not full AGCP commit-bound runtime governance because current canonical state and governing assumptions are not re-evaluated at commit.

Determination Rationale

Runtime Governance is assessed as Partial because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The target mediates proposed actions at runtime through a GovernanceEngine that validates envelopes, tenant state, provenance, policy applicability, and proposal-time invariants before issuing authorization or refusal outcomes.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Proposal-time governance mediation is implemented in executable code.
- Execution is gated by signed authorization reference validation.

Limitations

- Commit path omits current canonical-state re-evaluation.
- Authorization can remain usable after relevant resource assumptions change.

Procurement Implications

- Buyers may treat Runtime Governance as a partial feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

4.2.2 Governance Evidence

Field	Finding
Status / Assessment	Verified
Scope Classification	Core Scope
Confidence	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The target records governance activity in an append-only in-memory ledger with sequence numbers, previous hashes, event hashes, event types, timestamps, and event data. Proposal creation, refusals, approvals, authorizations, commit attempts, commits, and execution receipts produce evidence records.

Determination Rationale

Governance Evidence is assessed as Verified because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The target records governance activity in an append-only in-memory ledger with sequence numbers, previous hashes, event hashes, event types, timestamps, and event data.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Hash-linked ledger entries provide tamper-evidence for the synthetic execution history.
- Execution receipts and refusal records are explicit governance events.

Limitations

- Ledger is in-memory and not a durable production evidence store.
- Lifecycle state is maintained in mutable indexes rather than derived exclusively from the ledger.

Procurement Implications

- Buyers may treat Governance Evidence as a verified feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add retained tests and durable evidence artifacts if this capability is to be claimed beyond registry-assessment level.

4.2.3 Human Authorization Controls

Field	Finding
Status / Assessment	Partial
Scope Classification	Supporting Scope
Confidence	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The target supports human-in-the-loop approval for high-impact actions through PENDING_HITL lifecycle state, approval recording, quorum counting, invalid lifecycle rejection, and an invalid-signature branch. The capability is partial because approval signature verification is simulated by a boolean flag rather than a cryptographic approval artifact.

Determination Rationale

Human Authorization Controls is assessed as Partial because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The target supports human-in-the-loop approval for high-impact actions through PENDING_HITL lifecycle state, approval recording, quorum counting, invalid lifecycle rejection, and an invalid-signature branch.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Partial quorum accumulation and quorum completion are implemented.
- Invalid lifecycle and invalid signature branches exist.

Limitations

- No real cryptographic approval artifact is verified.
- No timeout, cancellation, or negative adjudication workflow is implemented.

Procurement Implications

- Buyers may treat Human Authorization Controls as a partial feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add retained tests and durable evidence artifacts if this capability is to be claimed beyond registry-assessment level.

4.2.4 Deterministic Governance

Field	Finding
Status / Assessment	Partial
Scope Classification	Supporting Scope
Confidence	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The target is deterministic for many static proposal-time inputs: equivalent proposal IDs and payloads replay existing outcomes, conflicting reused proposal IDs are rejected, and policy logic is explicit. Determinism is partial because wall-clock timestamps, UUID authorization identifiers, mutable state indexes, and token expiration prevent complete deterministic replay.

Determination Rationale

Deterministic Governance is assessed as Partial because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The target is deterministic for many static proposal-time inputs: equivalent proposal IDs and payloads replay existing outcomes, conflicting reused proposal IDs are rejected, and policy logic is explicit.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Proposal content hashing supports idempotent replay.
- Policy decisions are implemented as deterministic branches for static inputs.

Limitations

- Authorization IDs and timestamps are non-deterministic.
- Lifecycle state is mutable and not reconstructed solely from ordered history.

Procurement Implications

- Buyers may treat Deterministic Governance as a partial feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add retained tests and durable evidence artifacts if this capability is to be claimed beyond registry-assessment level.

4.2.5 Governance Continuity

Field	Finding
Status / Assessment	Partial
Scope Classification	Supporting Scope
Confidence	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The proposal envelope carries evidence references, provenance, context, target resource, actor identity, tenant identity, and intent through authorization issuance. Continuity is partial because these artifacts are not fully rebound and revalidated at commit.

Determination Rationale

Governance Continuity is assessed as Partial because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The proposal envelope carries evidence references, provenance, context, target resource, actor identity, tenant identity, and intent through authorization issuance.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Proposal, authorization, and ledger records maintain identifiers linking governance lifecycle events.
- Provenance hash and action hash bind some evaluated context into the authorization reference.

Limitations

- Execution does not re-check evidence references or provenance assumptions.
- No multi-agent or delegation continuity semantics are implemented.

Procurement Implications

- Buyers may treat Governance Continuity as a partial feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add retained tests and durable evidence artifacts if this capability is to be claimed beyond registry-assessment level.

4.2.6 Governance Degradation Management

Field	Finding
Status / Assessment	Partial
Scope Classification	Deferred
Confidence	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The target detects degraded-like conditions at submission, such as invalid provenance, inactive tenant state, schema defects, policy absence, and invariant failure. It does not implement a DEGRADED lifecycle state, post-authorization degradation detection, or mandatory re-evaluation after assumptions change.

Determination Rationale

Governance Degradation Management is assessed as Partial because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The target detects degraded-like conditions at submission, such as invalid provenance, inactive tenant state, schema defects, policy absence, and invariant failure.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Invalid provenance and tenant inactive states are refused at submission.
- Pending human review is represented as a non-terminal state.

Limitations

- No DEGRADED state exists.
- Stale authorizations after state changes are not degraded or refused before execution.

Procurement Implications

- Buyers may treat Governance Degradation Management as a partial feature for registry-style comparison, not as a verified or assured production claim.

- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

4.2.7 Multi-Agent Governance

Field	Finding
Status / Assessment	Not Present
Scope Classification	Outside Observed Scope
Confidence	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The target allows actor_type values such as agent, but it does not implement multi-agent coordination, agent handoff, cross-agent governance continuity, or distributed governance semantics. The capability is therefore not present in the observed implementation.

Determination Rationale

Multi-Agent Governance is assessed as Not Present because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The target allows actor_type values such as agent, but it does not implement multi-agent coordination, agent handoff, cross-agent governance continuity, or distributed governance semantics.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Agent-originated proposals can be represented.

Limitations

- No multi-agent coordination protocol exists.
- No agent handoff or delegated execution chain is modeled.

Procurement Implications

- Buyers may treat Multi-Agent Governance as a not present feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add retained tests and durable evidence artifacts if this capability is to be claimed beyond registry-assessment level.

4.2.8 Delegation Governance

Field	Finding
Status / Assessment	Not Present
Scope Classification	Outside Observed Scope
Confidence	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The target does not implement delegated authority chains or verifiable delegation semantics. It supports proposal actor identity and human approver identifiers, but no delegated authority model is implemented.

Determination Rationale

Delegation Governance is assessed as Not Present because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The target does not implement delegated authority chains or verifiable delegation semantics.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Actor and approver identifiers are captured.

Limitations

- Delegation boundaries and delegated authority proof are absent.

Procurement Implications

- Buyers may treat Delegation Governance as a not present feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add retained tests and durable evidence artifacts if this capability is to be claimed beyond registry-assessment level.

4.2.9 Tenant Isolation

Field	Finding
Status / Assessment	Partial
Scope Classification	Supporting Scope
Confidence	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The target is tenant-scoped in proposal submission and commit-token validation. Tenant identity appears in proposals and authorization references, and commit refuses mismatched tenant parameters. This is partial tenant isolation, not full tenant isolation across governance visibility, approvals, policy resolution, and ledger access.

Determination Rationale

Tenant Isolation is assessed as Partial because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The target is tenant-scoped in proposal submission and commit-token validation.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Tenant identifiers are included in proposal and authorization artifacts.
- Commit validates tenant match against authorization metadata.

Limitations

- No externally exposed cross-tenant read, approval, policy, or ledger access APIs are present for full isolation testing.
- Approver authority is not tenant-bound.

Procurement Implications

- Buyers may treat Tenant Isolation as a partial feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add retained tests and durable evidence artifacts if this capability is to be claimed beyond registry-assessment level.

4.2.10 Governance Auditability

Field	Finding
Status / Assessment	Verified
Scope Classification	Core Scope
Confidence	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	Primary implementation evidence for this capability.
specification	spec/architecture.md	Architectural description of the intended governance behavior and known limitations.

Narrative

The implementation produces ordered, hash-linked governance records for proposals, approvals, authorizations, refusals, commits, and execution receipts. This provides a clear audit trail for the synthetic package and supports reconstruction of observed events.

Determination Rationale

Governance Auditability is assessed as Verified because the inspected source and architecture demonstrate the behavior described above but the assessment does not infer capabilities beyond observable implementation evidence.

Evidence Analysis

Evidence was drawn from the executable GovernanceEngine, the architecture description, README, and retained pytest execution. The assessment treats implementation code and tests as higher weight than intended-result notes.

Architectural Observations

- The implementation produces ordered, hash-linked governance records for proposals, approvals, authorizations, refusals, commits, and execution receipts.
- The implementation is intentionally synthetic and optimized to illustrate buyer feature selection rather than production assurance.

Strengths

- Ledger events include sequence numbers and hash linkage.
- Refusals and execution receipts are recorded as governance outcomes.

Limitations

- Ledger storage is in-memory and not durable.
- Formal replay verification is not implemented as a separate API.

Procurement Implications

- Buyers may treat Governance Auditability as a verified feature for registry-style comparison, not as a verified or assured production claim.
- A Verified Assessment would require retained evidence, deeper test execution, and implementation-specific review.

Potential Expansion Approaches

- Add retained tests and durable evidence artifacts if this capability is to be claimed beyond registry-assessment level.

5 Semantic Equivalency Assessment

Semantic equivalency identifies conceptual alignment with AGCP independently from conformance, capability verification, registry eligibility, or procurement suitability.

5.1 Semantic Mapping

AGCP Concept	Equivalent Capability	Assessment
Governed Action Proposal	Structured proposal envelope with proposal_id, tenant_id, actor_id, action_type, target_resource, requested_effect, intent, evidence_refs, provenance, context, and expiration.	Strong
Governance Context Envelope	Context and provenance fields in the proposal envelope.	Partial
Canonical State Model	Mutable tenant and inventory dictionaries used during proposal-time evaluation.	Limited
Commit-Bound Execution Semantics	Execution gateway validates authorization token metadata but does not re-evaluate current canonical state.	Limited
Governance Receipt and Refusal Record Model	Hash-linked ledger events, Refusal records, Commit records, and ExecutionReceipt events.	Partial
HITL Governance	PENDING_HITL state, approvals list, quorum completion, invalid lifecycle rejection, and simulated signature-invalid rejection.	Partial
Tenant Isolation	Tenant IDs in proposals and authorization tokens with tenant match checking at commit.	Partial

5.2 AGCP-to-Target Schema Mapping

AGCP Element	Target Element	Mapping Type	Equivalency
Governed Action Proposal Schema	Proposal dictionary accepted by GovernanceEngine.submit	Direct	Strong
Governance Context Envelope	proposal.context plus provenance and evidence_refs	Partial	Partial
Canonical State Model	GovernanceEngine.tenants and GovernanceEngine.inventory mutable dictionaries	Conceptual	Limited
Authorization Artifact	authorization token dictionary with auth_id, proposal_id, tenant_id, action_hash, policy_version, provenance_hash, issued_at, expires_at, and HMAC signature	Direct	Strong

Continued on next page

AGCP Element	Target Element	Mapping Type	Equivalency
Commit-Bound Execution Semantics	GovernanceEngine.commit authorization-token validation path	Partial	Limited
Governance Receipt and Refusal Record Model	ledger entries including Refusal, Commit, and ExecutionReceipt events	Partial	Partial
DEGRADED Lifecycle State	No equivalent lifecycle state	No Equivalent	No Equivalent Capability

Schema Mapping Details

Governed Action Proposal Schema → Proposal dictionary accepted by GovernanceEngine.submit Evidence

- **source_file:** src/acme_governance/engine.py – REQUIRED_FIELDS defines the proposal envelope fields and submit enforces required-field presence.

Rationale

The target proposal object closely corresponds to an AGCP governed action proposal because it declares identity, tenant, action, target, requested effect, intent, evidence references, provenance, context, and expiration.

Limitations

- The proposal is represented as a Python dictionary rather than a normative AGCP schema artifact.

Governance Context Envelope → proposal.context plus provenance and evidence_refs Evidence

- **source_file:** src/acme_governance/engine.py – Proposal fields include context, evidence_refs, and provenance.

Rationale

The target carries context and provenance alongside the proposal, supporting governance coordination.

Limitations

- Context is not portable across agents or rebound at commit.
- Context is not distinguished from canonical state by an explicit schema.

Canonical State Model → GovernanceEngine.tenants and GovernanceEngine.inventory mutable dictionaries Evidence

- **source_file:** src/acme_governance/engine.py – The engine uses mutable dictionaries for tenant and inventory state during proposal-time evaluation.

Rationale

The target has operational state used for governance decisions, but it is mutable implementation state rather than an authoritative canonical-state model with replayable integrity.

Limitations

- State is not derived from append-only governance records.
- Commit does not re-resolve current canonical state.

Authorization Artifact → authorization token dictionary with auth_id, proposal_id, tenant_id, action_hash, policy_version, provenance_hash, issued_at, expires_at, and HMAC signature Evidence

- **source_file:** src/acme_governance/engine.py – _issue_authorization creates a signed authorization reference consumed by commit.

Rationale

The target authorization reference is a structured execution-gating artifact bound to proposal, tenant, action hash, policy version, provenance hash, and expiration metadata.

Limitations

- The token is not re-bound to current canonical state at commit.

Commit-Bound Execution Semantics → GovernanceEngine.commit authorization-token validation path Evidence

- **source_file:** src/acme_governance/engine.py – commit validates token metadata and then applies effect without re-running policy or canonical-state checks.
- **test_case:** tests/test_intended_assessment_behavior.py – The stale authorization test proves commit succeeds after inventory assumptions are invalidated.

Rationale

The target has an execution gate, but the gate validates historical authorization metadata rather than performing commit-bound admissibility evaluation.

Limitations

- No current-state re-evaluation.
- No governing-assumption rebinding.
- Stale authorization may execute.

Governance Receipt and Refusal Record Model → ledger entries including Refusal, Commit, and ExecutionReceipt events Evidence

- **source_file:** src/acme_governance/engine.py – _record creates hash-linked ledger entries for governance events.

Rationale

The target treats refusals and execution receipts as explicit events and records them in the governance ledger.

Limitations

- Ledger is in-memory.
- Receipts are not formal AGCP receipt artifacts.

DEGRADED Lifecycle State → No equivalent lifecycle state Evidence

- **source_file:** src/acme_governance/engine.py – ProposalRecord.status supports observed states such as AUTHORIZED, PENDING_HITL, REJECTED, and EXECUTED but no DEGRADED state is implemented.

Rationale

The target refuses some invalid proposals at submission but does not represent degraded post-authorization lifecycle status.

Limitations

- No degradation state transition or retention decision exists.

5.3 Semantic Equivalency Summary

Category	Assessment
Strong Equivalency	Proposal envelope, authorization artifact, provenance validation, and audit event concepts.
Partial Equivalency	Governance context, HITL, tenant scoping, refusal records, and deterministic proposal-time behavior.
Limited Equivalency	Canonical state, commit-bound execution semantics, replay verification, and lifecycle derivation.
No Equivalent Capability	DEGRADED lifecycle semantics, multi-agent governance continuity, delegated authority verification, and cross-implementation semantic equivalence.

5.4 Major Alignment Areas

- **Proposal and authorization artifacts:** The target has explicit proposal dictionaries and signed authorization references.
- **Governance evidence:** Hash-linked ledger events preserve governance history for the synthetic engine.

5.5 Major Divergence Areas

- **Commit-bound admissibility:** The commit gateway validates historical authorization token metadata rather than current canonical state.
- **Lifecycle derivation:** Lifecycle status is mutable in ProposalRecord rather than derived solely from ledger history.

5.6 Architectural Divergences

The target implements a common enterprise pattern: proposal-time policy evaluation and token-gated execution. AGCP requires stronger commit-bound admissibility, canonical-state resolution, and lifecycle derivation at the execution boundary.

5.7 Interpretation

The target is semantically close enough to AGCP concepts to support meaningful registry characterization, but not close enough to claim full AGCP conformance.

6 AGCP Conformance Assessment

Conformance findings evaluate the target against AGCP requirements. Scope interpretation explains whether a non-demonstrated requirement appears central, supporting, deferred, outside observed scope, or unknown.

6.1 Requirement Summary Matrix

Requirement	Level	Result	Confidence	Summary
CR-001	L2 — Ordered Governance Mediation	Pass	High	Observed evidence directly supports the requirement: A proposal that satisfies all governance constraints SHALL be eligible for authorization.
CR-002	L4 — Execution Authorization Control	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evaluation SHALL support escalation and deferred human adjudication paths.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-003	L2 — Ordered Governance Mediation	Pass	High	Observed evidence directly supports the requirement: Actions that violate mandatory invariants SHALL NOT be authorized.
CR-004	L1 — Schema & Envelope Validation	Pass	High	Observed evidence directly supports the requirement: Governance evaluation SHALL reject structurally invalid proposals.
CR-005	L1 — Schema & Envelope Validation	Pass	High	Observed evidence directly supports the requirement: Governance decisions SHALL require verifiable provenance where mandated.
CR-006	L2 — Ordered Governance Mediation	Pass	High	Observed evidence directly supports the requirement: Governance evaluation SHALL enforce tenant operational status constraints.
CR-007	L2 — Ordered Governance Mediation	Pass	High	Observed evidence directly supports the requirement: Authorization SHALL require an applicable governance policy.
CR-008	L3 — Deterministic Governance	Pass	High	Observed evidence directly supports the requirement: Equivalent requests SHALL produce deterministic governance outcomes.
CR-009	L3 — Deterministic Governance	Pass	High	Observed evidence directly supports the requirement: Non-equivalent requests SHALL NOT share governance identity.
CR-010	L1 — Schema & Envelope Validation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Authorized governance state SHALL be externally retrievable.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-011	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Internal processing states SHALL NOT become canonical externally visible governance states.
CR-012	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Governance escalation SHALL support partial quorum accumulation.
CR-013	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Required governance quorum satisfaction SHALL enable authorization.
CR-014	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Human authorization artifacts SHALL only apply to eligible lifecycle states.
CR-015	L4 — Execution Authorization Control	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Expired governance approvals SHALL NOT remain valid.
CR-016	L4 — Execution Authorization Control	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance approvals SHALL be cryptographically attributable and verifiable.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-017	L4 — Execution Authorization Control	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Unresolved escalations SHALL terminate according to governance policy.
CR-018	L4 — Execution Authorization Control	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance authorities SHALL be able to terminate pending actions.
CR-019	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Operational realization SHALL occur only after successful authorization.
CR-020	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Pending governance evaluation SHALL NOT permit execution.
CR-021	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Rejected actions SHALL NOT become operationally real.
CR-022	L4 — Execution Authorization Control	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Execution SHALL remain bound to the specific authorization artifact that approved it.
CR-023	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Executed actions SHALL be terminal and non-repeatable.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-024	L4 — Execution Authorization Control	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Commit admissibility SHALL be evaluated against current governance reality.
CR-025	L4 — Execution Authorization Control	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance authority SHALL terminate when governance subjects cease to exist.
CR-026	L5 — Multi-tenant Governance Isolation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance visibility SHALL respect tenant isolation boundaries.
CR-027	L5 — Multi-tenant Governance Isolation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance authority SHALL NOT cross tenant boundaries.
CR-028	L5 — Multi-tenant Governance Isolation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Execution authority SHALL NOT cross tenant boundaries.
CR-029	L5 — Multi-tenant Governance Isolation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance policy scope SHALL be tenant-isolated.
CR-030	L5 — Multi-tenant Governance Isolation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance evidence SHALL be tenant-isolated.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-031	L4 — Execution Authorization Control	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Authorization SHALL NOT imply unconditional future execution authority.
CR-032	L4	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Commit admissibility SHALL be derived from current canonical state, not historical authorization alone.
CR-033	L4	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Execution authority SHALL remain valid only while its governing assumptions remain valid.
CR-034	L3 — Deterministic Governance	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance outcomes SHALL remain consistent under concurrent evaluation.
CR-035	L4	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Escalated actions SHALL be re-evaluated against current canonical state before execution.
CR-036	L1 — Schema & Envelope Validation	Pass	High	Observed evidence directly supports the requirement: Governed proposals SHALL declare operational intent.
CR-037	L1	Pass	High	Observed evidence directly supports the requirement: Governed proposals SHALL identify the object of governance action.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-038	L1	Pass	High	Observed evidence directly supports the requirement: Governed proposals SHALL declare intended operational effect.
CR-039	L1	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance requests SHALL respect temporal validity constraints.
CR-040	L1	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Delegated governance authority SHALL be verifiable.
CR-041	L1 — Schema & Envelope Validation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evidence references SHALL be resolvable and verifiable.
CR-042	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance objects SHALL support deterministic replay integrity.
CR-043	L1 — Schema & Envelope Validation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance context SHALL preserve operational lineage when required.
CR-044	L2 — Ordered Governance Mediation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance continuity SHALL be preserved across delegation boundaries.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-045	L1 — Schema & Envelope Validation	Pass	High	Observed evidence directly supports the requirement: Governance attribution SHALL remain consistent and unambiguous.
CR-046	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance context SHALL NOT supersede canonical governance reality.
CR-047	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance provenance SHALL remain continuous across lifecycle transitions.
CR-048	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Commit decisions SHALL require authoritative governance state.
CR-049	L3 — Deterministic Governance	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance evaluation SHALL use sufficiently current canonical state.
CR-050	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evaluation SHALL resolve a single authoritative state.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-051	L3 — Deterministic Governance	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Canonical state SHALL take precedence over non-authoritative observations.
CR-052	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Canonical-state integrity SHALL be verifiable and replayable.
CR-053	L2 — Ordered Governance Mediation	Pass	High	Observed evidence directly supports the requirement: Inadmissible actions SHALL be structurally refused.
CR-054	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Evidence insufficiency SHALL prevent authorization.
CR-055	L3 — Deterministic Governance	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance conflicts SHALL prevent operational realization.
CR-056	L2 — Ordered Governance Mediation	Pass	High	Observed evidence directly supports the requirement: Refusals SHALL be attributable governance outcomes.
CR-057	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Refusals SHALL be reconstructable and replayable.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-058	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Escalation decisions SHALL be evidenced.
CR-059	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Escalation outcomes SHALL integrate into lifecycle progression.
CR-060	L4 — Execution Authorization Control	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Escalation outcomes SHALL support negative adjudication.
CR-061	L4 — Execution Authorization Control	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Deferred governance decisions SHALL honor validity periods.
CR-062	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL reference governing state.
CR-063	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL identify governing constraints.
CR-064	L2 — Ordered Governance Mediation	Pass	High	Observed evidence directly supports the requirement: Governance outcomes SHALL preserve evidence integrity.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-065	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL be attributable to accountable actors.
CR-066	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL support replay verification.
CR-067	L3 — Deterministic Governance	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance evidence SHALL remain consistent across evaluation and execution.
CR-068	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Commit decisions SHALL remain supportable by evidence.
CR-069	L2 — Ordered Governance Mediation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Evidence continuity SHALL survive multi-agent workflows.
CR-070	L2 — Ordered Governance Mediation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance continuity SHALL survive agent handoffs.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-071	L2 — Ordered Governance Mediation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Agents SHALL preserve required governance context.
CR-072	L4 — Execution Authorization Control	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance-domain transitions SHALL remain governed.
CR-073	L3 — Deterministic Governance	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance semantics SHALL be transport-independent.
CR-074	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evaluation SHALL be semantically deterministic.
CR-075	L3 — Deterministic Governance	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Conformant implementations SHALL produce equivalent governance outcomes.
CR-076	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evaluation SHALL be deterministic.
CR-077	L3 — Deterministic Governance	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance evaluation SHALL be node-independent.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-078	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL be independent of internal agent reasoning variability.
CR-079	L4 — Execution Authorization Control	Pass	High	Observed evidence directly supports the requirement: Governance SHALL correctly admit admissible actions.
CR-080	L4 — Execution Authorization Control	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance SHALL correctly reject inadmissible actions.
CR-081	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance lifecycle progression SHALL preserve lifecycle integrity.
CR-082	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance state SHALL be derivable from governance records.
CR-083	L3 — Deterministic Governance	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance decisions SHALL remain synchronized with authoritative state.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-084	L4 — Execution Authorization Control	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Admissibility SHALL be commit-bound.
CR-085	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance decisions SHALL be replayable.
CR-086	L3 — Deterministic Governance	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL support independent verification.
CR-087	L2 — Ordered Governance Mediation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance SHALL reliably detect inadmissibility.
CR-088	L4 — Execution Authorization Control	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Structural refusal SHALL be enforceable.
CR-089	L5 — Multi-tenant Governance Isolation	Partial	Medium	The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Implementations SHALL conform to AGCP governance semantics.

Continued on next page

Requirement	Level	Result	Confidence	Summary
CR-090	L5 — Multi-tenant Governance Isolation	Not Assessed	Medium	Available evidence was insufficient to assess this requirement directly: Governance semantics SHALL be interoperable and semantically equivalent across implementations.
CR-091	L2 — Ordered Governance Mediation	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: A governance object SHALL enter DEGRADED state when one or more governance assumptions, evidence artifacts, contextual dependencies, authorization conditions, or canonical-state dependencies required for continued admissibility can no longer be verified.
CR-092	L2 — Ordered Governance Mediation	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: DEGRADED SHALL be a non-terminal lifecycle state.
CR-093	L4 — Execution Authorization Control	Fail	High	Observable source evidence shows the required behavior is absent or intentionally not implemented: Objects in DEGRADED state SHALL require re-evaluation prior to authorization retention or execution.

6.2 Detailed Requirement Findings

6.2.1 CR-001 - A proposal that satisfies all governance constraints SHALL be eligible for authorization.

Field	Finding
Requirement Identifier	CR-001
Requirement Name	A proposal that satisfies all governance constraints SHALL be eligible for authorization.
Normative Requirement	A proposal that satisfies all governance constraints SHALL be eligible for authorization.
Conformance Level	L2 — Ordered Governance Mediation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: A proposal that satisfies all governance constraints SHALL be eligible for authorization.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.2 CR-002 - Governance evaluation SHALL support escalation and deferred human adjudication paths.

Field	Finding
Requirement Identifier	CR-002
Requirement Name	Governance evaluation SHALL support escalation and deferred human adjudication paths.
Normative Requirement	Governance evaluation SHALL support escalation and deferred human adjudication paths.
Conformance Level	L4 — Execution Authorization Control
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evaluation SHALL support escalation and deferred human adjudication paths.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.3 CR-003 - Actions that violate mandatory invariants SHALL NOT be authorized.

Field	Finding
Requirement Identifier	CR-003
Requirement Name	Actions that violate mandatory invariants SHALL NOT be authorized.
Normative Requirement	Actions that violate mandatory invariants SHALL NOT be authorized.
Conformance Level	L2 — Ordered Governance Mediation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Actions that violate mandatory invariants SHALL NOT be authorized.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.4 CR-004 - Governance evaluation SHALL reject structurally invalid proposals.

Field	Finding
Requirement Identifier	CR-004
Requirement Name	Governance evaluation SHALL reject structurally invalid proposals.
Normative Requirement	Governance evaluation SHALL reject structurally invalid proposals.
Conformance Level	L1 — Schema & Envelope Validation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
test_case	tests/test_intended_assessment_behavior.py	The pytest suite directly exercises schema rejection, provenance rejection, authorized commit, HITL gating, and the intentional stale-authorization commit gap.

Summary

Observed evidence directly supports the requirement: Governance evaluation SHALL reject structurally invalid proposals.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.5 CR-005 - Governance decisions SHALL require verifiable provenance where mandated.

Field	Finding
Requirement Identifier	CR-005
Requirement Name	Governance decisions SHALL require verifiable provenance where mandated.
Normative Requirement	Governance decisions SHALL require verifiable provenance where mandated.
Conformance Level	L1 — Schema & Envelope Validation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
test_case	tests/test_intended_assessment_behavior.py:1	The pytest suite directly exercises schema rejection, provenance rejection, authorized commit, HITL gating, and the intentional stale-authorization commit gap.

Summary

Observed evidence directly supports the requirement: Governance decisions SHALL require verifiable provenance where mandated.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.6 CR-006 - Governance evaluation SHALL enforce tenant operational status constraints.

Field	Finding
Requirement Identifier	CR-006
Requirement Name	Governance evaluation SHALL enforce tenant operational status constraints.
Normative Requirement	Governance evaluation SHALL enforce tenant operational status constraints.
Conformance Level	L2 — Ordered Governance Mediation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Governance evaluation SHALL enforce tenant operational status constraints.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.7 CR-007 - Authorization SHALL require an applicable governance policy.

Field	Finding
Requirement Identifier	CR-007
Requirement Name	Authorization SHALL require an applicable governance policy.
Normative Requirement	Authorization SHALL require an applicable governance policy.
Conformance Level	L2 — Ordered Governance Mediation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Authorization SHALL require an applicable governance policy.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.8 CR-008 - Equivalent requests SHALL produce deterministic governance outcomes.

Field	Finding
Requirement Identifier	CR-008
Requirement Name	Equivalent requests SHALL produce deterministic governance outcomes.
Normative Requirement	Equivalent requests SHALL produce deterministic governance outcomes.
Conformance Level	L3 — Deterministic Governance
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Equivalent requests SHALL produce deterministic governance outcomes.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.9 CR-009 - Non-equivalent requests SHALL NOT share governance identity.

Field	Finding
Requirement Identifier	CR-009
Requirement Name	Non-equivalent requests SHALL NOT share governance identity.
Normative Requirement	Non-equivalent requests SHALL NOT share governance identity.
Conformance Level	L3 — Deterministic Governance
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Non-equivalent requests SHALL NOT share governance identity.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.10 CR-010 - Authorized governance state SHALL be externally retrievable.

Field	Finding
Requirement Identifier	CR-010
Requirement Name	Authorized governance state SHALL be externally retrievable.
Normative Requirement	Authorized governance state SHALL be externally retrievable.
Conformance Level	L1 — Schema & Envelope Validation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
repository_location	acme_supply_ai_execution_governance_architecture	No clear executable or artifact-level evidence was found for this AGCP requirement in the synthetic target package.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Authorized governance state SHALL be externally retrievable.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.11 CR-011 - Internal processing states SHALL NOT become canonical externally visible governance states.

Field	Finding
Requirement Identifier	CR-011
Requirement Name	Internal processing states SHALL NOT become canonical externally visible governance states.
Normative Requirement	Internal processing states SHALL NOT become canonical externally visible governance states.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
repository_location	acme_supply_ai_execution_governance_architecture	No clear executable or artifact-level evidence was found for this AGCP requirement in the synthetic target package.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Internal processing states SHALL NOT become canonical externally visible governance states.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.12 CR-012 - Governance escalation SHALL support partial quorum accumulation.

Field	Finding
Requirement Identifier	CR-012
Requirement Name	Governance escalation SHALL support partial quorum accumulation.
Normative Requirement	Governance escalation SHALL support partial quorum accumulation.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

Observed evidence directly supports the requirement: Governance escalation SHALL support partial quorum accumulation.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.13 CR-013 - Required governance quorum satisfaction SHALL enable authorization.

Field	Finding
Requirement Identifier	CR-013
Requirement Name	Required governance quorum satisfaction SHALL enable authorization.
Normative Requirement	Required governance quorum satisfaction SHALL enable authorization.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

Observed evidence directly supports the requirement: Required governance quorum satisfaction SHALL enable authorization.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.14 CR-014 - Human authorization artifacts SHALL only apply to eligible lifecycle states.

Field	Finding
Requirement Identifier	CR-014
Requirement Name	Human authorization artifacts SHALL only apply to eligible lifecycle states.
Normative Requirement	Human authorization artifacts SHALL only apply to eligible lifecycle states.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

Observed evidence directly supports the requirement: Human authorization artifacts SHALL only apply to eligible lifecycle states.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.15 CR-015 - Expired governance approvals SHALL NOT remain valid.

Field	Finding
Requirement Identifier	CR-015
Requirement Name	Expired governance approvals SHALL NOT remain valid.
Normative Requirement	Expired governance approvals SHALL NOT remain valid.
Conformance Level	L4 — Execution Authorization Control
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Expired governance approvals SHALL NOT remain valid.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.16 CR-016 - Governance approvals SHALL be cryptographically attributable and verifiable.

Field	Finding
Requirement Identifier	CR-016
Requirement Name	Governance approvals SHALL be cryptographically attributable and verifiable.
Normative Requirement	Governance approvals SHALL be cryptographically attributable and verifiable.
Conformance Level	L4 — Execution Authorization Control
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance approvals SHALL be cryptographically attributable and verifiable.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

The approval API supports an invalid-signature rejection branch, but the approval artifact itself is represented by a boolean flag rather than a cryptographically verified signer artifact. This supports a partial finding rather than full cryptographic approval verification.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Replace simulated approval flags with verifiable approval artifacts, explicit expiration, cancellation, timeout, and negative-adjudication handling.
- Retain approval and escalation evidence as structured governance records.

6.2.17 CR-017 - Unresolved escalations SHALL terminate according to governance policy.

Field	Finding
Requirement Identifier	CR-017
Requirement Name	Unresolved escalations SHALL terminate according to governance policy.
Normative Requirement	Unresolved escalations SHALL terminate according to governance policy.
Conformance Level	L4 — Execution Authorization Control
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Unresolved escalations SHALL terminate according to governance policy.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The source evidence is negative evidence: the package intentionally omits the required behavior, or the tests demonstrate behavior that would be refused by a fully commit-bound AGCP implementation.

Architectural Interpretation

The implementation architecture intentionally stops short of the normative AGCP behavior.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Replace simulated approval flags with verifiable approval artifacts, explicit expiration, cancellation, timeout, and negative-adjudication handling.
- Retain approval and escalation evidence as structured governance records.

6.2.18 CR-018 - Governance authorities SHALL be able to terminate pending actions.

Field	Finding
Requirement Identifier	CR-018
Requirement Name	Governance authorities SHALL be able to terminate pending actions.
Normative Requirement	Governance authorities SHALL be able to terminate pending actions.
Conformance Level	L4 — Execution Authorization Control
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance authorities SHALL be able to terminate pending actions.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The source evidence is negative evidence: the package intentionally omits the required behavior, or the tests demonstrate behavior that would be refused by a fully commit-bound AGCP implementation.

Architectural Interpretation

The implementation architecture intentionally stops short of the normative AGCP behavior.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Replace simulated approval flags with verifiable approval artifacts, explicit expiration, cancellation, timeout, and negative-adjudication handling.
- Retain approval and escalation evidence as structured governance records.

6.2.19 CR-019 - Operational realization SHALL occur only after successful authorization.

Field	Finding
Requirement Identifier	CR-019
Requirement Name	Operational realization SHALL occur only after successful authorization.
Normative Requirement	Operational realization SHALL occur only after successful authorization.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
test_case	tests/test_intended_assessment_behavior.py	The pytest suite directly exercises schema rejection, provenance rejection, authorized commit, HITL gating, and the intentional stale-authorization commit gap.

Summary

Observed evidence directly supports the requirement: Operational realization SHALL occur only after successful authorization.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.20 CR-020 - Pending governance evaluation SHALL NOT permit execution.

Field	Finding
Requirement Identifier	CR-020
Requirement Name	Pending governance evaluation SHALL NOT permit execution.
Normative Requirement	Pending governance evaluation SHALL NOT permit execution.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
test_case	tests/test_intended_assessment_behavior.py	The pytest suite directly exercises schema rejection, provenance rejection, authorized commit, HITL gating, and the intentional stale-authorization commit gap.

Summary

Observed evidence directly supports the requirement: Pending governance evaluation SHALL NOT permit execution.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.21 CR-021 - Rejected actions SHALL NOT become operationally real.

Field	Finding
Requirement Identifier	CR-021
Requirement Name	Rejected actions SHALL NOT become operationally real.
Normative Requirement	Rejected actions SHALL NOT become operationally real.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.

Summary

Observed evidence directly supports the requirement: Rejected actions SHALL NOT become operationally real.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.22 CR-022 - Execution SHALL remain bound to the specific authorization artifact that approved it.

Field	Finding
Requirement Identifier	CR-022
Requirement Name	Execution SHALL remain bound to the specific authorization artifact that approved it.
Normative Requirement	Execution SHALL remain bound to the specific authorization artifact that approved it.
Conformance Level	L4 — Execution Authorization Control
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Execution SHALL remain bound to the specific authorization artifact that approved it.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.23 CR-023 - Executed actions SHALL be terminal and non-repeatable.

Field	Finding
Requirement Identifier	CR-023
Requirement Name	Executed actions SHALL be terminal and non-repeatable.
Normative Requirement	Executed actions SHALL be terminal and non-repeatable.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.

Summary

Observed evidence directly supports the requirement: Executed actions SHALL be terminal and non-repeatable.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.24 CR-024 - Commit admissibility SHALL be evaluated against current governance reality.

Field	Finding
Requirement Identifier	CR-024
Requirement Name	Commit admissibility SHALL be evaluated against current governance reality.
Normative Requirement	Commit admissibility SHALL be evaluated against current governance reality.
Conformance Level	L4 — Execution Authorization Control
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Commit admissibility SHALL be evaluated against current governance reality.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The strongest evidence is the commit implementation and the documented stale-authorization scenario. The commit path validates token metadata and lifecycle status, then applies the effect without re-resolving current inventory or other authoritative state. The pytest suite confirms that a second stale inventory authorization can still commit.

Architectural Interpretation

Architecturally, this is the key distinction between provenance-rich proposal-time authorization and commit-bound AGCP admissibility. The target uses authorization tokens as the execution gate but does not make current canonical state the binding authority at commit.

Buyer Implications

Buyers should treat this as suitable for illustrating proposal-time governance and authorization-token gating, not as evidence of commit-bound runtime admissibility for stale or conflicting actions.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.25 CR-025 - Governance authority SHALL terminate when governance subjects cease to exist.

Field	Finding
Requirement Identifier	CR-025
Requirement Name	Governance authority SHALL terminate when governance subjects cease to exist.
Normative Requirement	Governance authority SHALL terminate when governance subjects cease to exist.
Conformance Level	L4 — Execution Authorization Control
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance authority SHALL terminate when governance subjects cease to exist.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The source evidence is negative evidence: the package intentionally omits the required behavior, or the tests demonstrate behavior that would be refused by a fully commit-bound AGCP implementation.

Architectural Interpretation

The implementation architecture intentionally stops short of the normative AGCP behavior.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.26 CR-026 - Governance visibility SHALL respect tenant isolation boundaries.

Field	Finding
Requirement Identifier	CR-026
Requirement Name	Governance visibility SHALL respect tenant isolation boundaries.
Normative Requirement	Governance visibility SHALL respect tenant isolation boundaries.
Conformance Level	L5 — Multitenant Governance Isolation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Unknown

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance visibility SHALL respect tenant isolation boundaries.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

Tenant identifiers exist and the commit path checks tenant match against authorization metadata, but the repository lacks externally exposed read, approval-authority, policy-resolution, and ledger-access APIs needed to verify the full tenant-isolation surface.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Expose tenant-scoped read, approval, policy-resolution, and ledger-access APIs and test cross-tenant refusal paths.
- Bind tenant authority to authenticated actor identity rather than relying only on request parameters.

6.2.27 CR-027 - Governance authority SHALL NOT cross tenant boundaries.

Field	Finding
Requirement Identifier	CR-027
Requirement Name	Governance authority SHALL NOT cross tenant boundaries.
Normative Requirement	Governance authority SHALL NOT cross tenant boundaries.
Conformance Level	L5 — Multitenant Governance Isolation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Unknown

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance authority SHALL NOT cross tenant boundaries.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

Tenant identifiers exist and the commit path checks tenant match against authorization metadata, but the repository lacks externally exposed read, approval-authority, policy-resolution, and ledger-access APIs needed to verify the full tenant-isolation surface.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Expose tenant-scoped read, approval, policy-resolution, and ledger-access APIs and test cross-tenant refusal paths.
- Bind tenant authority to authenticated actor identity rather than relying only on request parameters.

6.2.28 CR-028 - Execution authority SHALL NOT cross tenant boundaries.

Field	Finding
Requirement Identifier	CR-028
Requirement Name	Execution authority SHALL NOT cross tenant boundaries.
Normative Requirement	Execution authority SHALL NOT cross tenant boundaries.
Conformance Level	L5 — Multitenant Governance Isolation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Execution authority SHALL NOT cross tenant boundaries.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.29 CR-029 - Governance policy scope SHALL be tenant-isolated.

Field	Finding
Requirement Identifier	CR-029
Requirement Name	Governance policy scope SHALL be tenant-isolated.
Normative Requirement	Governance policy scope SHALL be tenant-isolated.
Conformance Level	L5 — Multitenant Governance Isolation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Unknown

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance policy scope SHALL be tenant-isolated.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

Tenant identifiers exist and the commit path checks tenant match against authorization metadata, but the repository lacks externally exposed read, approval-authority, policy-resolution, and ledger-access APIs needed to verify the full tenant-isolation surface.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Expose tenant-scoped read, approval, policy-resolution, and ledger-access APIs and test cross-tenant refusal paths.
- Bind tenant authority to authenticated actor identity rather than relying only on request parameters.

6.2.30 CR-030 - Governance evidence SHALL be tenant-isolated.

Field	Finding
Requirement Identifier	CR-030
Requirement Name	Governance evidence SHALL be tenant-isolated.
Normative Requirement	Governance evidence SHALL be tenant-isolated.
Conformance Level	L5 — Multitenant Governance Isolation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Unknown

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance evidence SHALL be tenant-isolated.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

Tenant identifiers exist and the commit path checks tenant match against authorization metadata, but the repository lacks externally exposed read, approval-authority, policy-resolution, and ledger-access APIs needed to verify the full tenant-isolation surface.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Expose tenant-scoped read, approval, policy-resolution, and ledger-access APIs and test cross-tenant refusal paths.
- Bind tenant authority to authenticated actor identity rather than relying only on request parameters.

6.2.31 CR-031 - Authorization SHALL NOT imply unconditional future execution authority.

Field	Finding
Requirement Identifier	CR-031
Requirement Name	Authorization SHALL NOT imply unconditional future execution authority.
Normative Requirement	Authorization SHALL NOT imply unconditional future execution authority.
Conformance Level	L4 — Execution Authorization Control
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Authorization SHALL NOT imply unconditional future execution authority.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The strongest evidence is the commit implementation and the documented stale-authorization scenario. The commit path validates token metadata and lifecycle status, then applies the effect without re-resolving current inventory or other authoritative state. The pytest suite confirms that a second stale inventory authorization can still commit.

Architectural Interpretation

Architecturally, this is the key distinction between provenance-rich proposal-time authorization and commit-bound AGCP admissibility. The target uses authorization tokens as the execution gate but does not make current canonical state the binding authority at commit.

Buyer Implications

Buyers should treat this as suitable for illustrating proposal-time governance and authorization-token gating, not as evidence of commit-bound runtime admissibility for stale or conflicting actions.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.32 CR-032 - Commit admissibility SHALL be derived from current canonical state, not historical authorization alone.

Field	Finding
Requirement Identifier	CR-032
Requirement Name	Commit admissibility SHALL be derived from current canonical state, not historical authorization alone.
Normative Requirement	Commit admissibility SHALL be derived from current canonical state, not historical authorization alone.
Conformance Level	L4
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
test_case	tests/test_intended_assessment_behavior.py	The pytest suite directly exercises schema rejection, provenance rejection, authorized commit, HITL gating, and the intentional stale-authorization commit gap.
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Commit admissibility SHALL be derived from current canonical state, not historical authorization alone.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The strongest evidence is the commit implementation and the documented stale-authorization scenario. The commit path validates token metadata and lifecycle status, then applies the effect without re-resolving current inventory or other authoritative state. The pytest suite confirms that a second stale inventory authorization can still commit.

Architectural Interpretation

Architecturally, this is the key distinction between provenance-rich proposal-time authorization and commit-bound AGCP admissibility. The target uses authorization tokens as the execution gate but does not make current canonical state the binding authority at commit.

Buyer Implications

Buyers should treat this as suitable for illustrating proposal-time governance and authorization-token gating, not as evidence of commit-bound runtime admissibility for stale or conflicting actions.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.33 CR-033 - Execution authority SHALL remain valid only while its governing assumptions remain valid.

Field	Finding
Requirement Identifier	CR-033
Requirement Name	Execution authority SHALL remain valid only while its governing assumptions remain valid.
Normative Requirement	Execution authority SHALL remain valid only while its governing assumptions remain valid.
Conformance Level	L4
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Execution authority SHALL remain valid only while its governing assumptions remain valid.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The strongest evidence is the commit implementation and the documented stale-authorization scenario. The commit path validates token metadata and lifecycle status, then applies the effect without re-resolving current inventory or other authoritative state. The pytest suite confirms that a second stale inventory authorization can still commit.

Architectural Interpretation

Architecturally, this is the key distinction between provenance-rich proposal-time authorization and commit-bound AGCP admissibility. The target uses authorization tokens as the execution gate but does not make current canonical state the binding authority at commit.

Buyer Implications

Buyers should treat this as suitable for illustrating proposal-time governance and authorization-token gating, not as evidence of commit-bound runtime admissibility for stale or conflicting actions.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.34 CR-034 - Governance outcomes SHALL remain consistent under concurrent evaluation.

Field	Finding
Requirement Identifier	CR-034
Requirement Name	Governance outcomes SHALL remain consistent under concurrent evaluation.
Normative Requirement	Governance outcomes SHALL remain consistent under concurrent evaluation.
Conformance Level	L3 — Deterministic Governance
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Unknown

Evidence

Type	Location	Rationale
repository_location	acme_supply_ai_execution_governance_architecture	No directly observable or artifact-level evidence was found for this AGCP requirement in the synthetic target package.

Summary

Available evidence was insufficient to assess this requirement directly: Governance outcomes SHALL remain consistent under concurrent evaluation.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.35 CR-035 - Escalated actions SHALL be re-evaluated against current canonical state before execution.

Field	Finding
Requirement Identifier	CR-035
Requirement Name	Escalated actions SHALL be re-evaluated against current canonical state before execution.
Normative Requirement	Escalated actions SHALL be re-evaluated against current canonical state before execution.
Conformance Level	L4
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Type	Location	Rationale
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Escalated actions SHALL be re-evaluated against current canonical state before execution.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The strongest evidence is the commit implementation and the documented stale-authorization scenario. The commit path validates token metadata and lifecycle status, then applies the effect without re-resolving current inventory or other authoritative state. The pytest suite confirms that a second stale inventory authorization can still commit.

Architectural Interpretation

Architecturally, this is the key distinction between provenance-rich proposal-time authorization and commit-bound AGCP admissibility. The target uses authorization tokens as the execution gate but does not make current canonical state the binding authority at commit.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.

- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.36 CR-036 - Governed proposals SHALL declare operational intent.

Field	Finding
Requirement Identifier	CR-036
Requirement Name	Governed proposals SHALL declare operational intent.
Normative Requirement	Governed proposals SHALL declare operational intent.
Conformance Level	L1 — Schema & Envelope Validation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Governed proposals SHALL declare operational intent.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.37 CR-037 - Governed proposals SHALL identify the object of governance action.

Field	Finding
Requirement Identifier	CR-037
Requirement Name	Governed proposals SHALL identify the object of governance action.
Normative Requirement	Governed proposals SHALL identify the object of governance action.
Conformance Level	L1
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Governed proposals SHALL identify the object of governance action.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.38 CR-038 - Governed proposals SHALL declare intended operational effect.

Field	Finding
Requirement Identifier	CR-038
Requirement Name	Governed proposals SHALL declare intended operational effect.
Normative Requirement	Governed proposals SHALL declare intended operational effect.
Conformance Level	L1
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Governed proposals SHALL declare intended operational effect.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.39 CR-039 - Governance requests SHALL respect temporal validity constraints.

Field	Finding
Requirement Identifier	CR-039
Requirement Name	Governance requests SHALL respect temporal validity constraints.
Normative Requirement	Governance requests SHALL respect temporal validity constraints.
Conformance Level	L1
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance requests SHALL respect temporal validity constraints.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.40 CR-040 - Delegated governance authority SHALL be verifiable.

Field	Finding
Requirement Identifier	CR-040
Requirement Name	Delegated governance authority SHALL be verifiable.
Normative Requirement	Delegated governance authority SHALL be verifiable.
Conformance Level	L1
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Delegated governance authority SHALL be verifiable.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.41 CR-041 - Governance evidence references SHALL be resolvable and verifiable.

Field	Finding
Requirement Identifier	CR-041
Requirement Name	Governance evidence references SHALL be resolvable and verifiable.
Normative Requirement	Governance evidence references SHALL be resolvable and verifiable.
Conformance Level	L1 — Schema & Envelope Validation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evidence references SHALL be resolvable and verifiable.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.42 CR-042 - Governance objects SHALL support deterministic replay integrity.

Field	Finding
Requirement Identifier	CR-042
Requirement Name	Governance objects SHALL support deterministic replay integrity.
Normative Requirement	Governance objects SHALL support deterministic replay integrity.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance objects SHALL support deterministic replay integrity.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.43 CR-043 - Governance context SHALL preserve operational lineage when required.

Field	Finding
Requirement Identifier	CR-043
Requirement Name	Governance context SHALL preserve operational lineage when required.
Normative Requirement	Governance context SHALL preserve operational lineage when required.
Conformance Level	L1 — Schema & Envelope Validation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance context SHALL preserve operational lineage when required.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.44 CR-044 - Governance continuity SHALL be preserved across delegation boundaries.

Field	Finding
Requirement Identifier	CR-044
Requirement Name	Governance continuity SHALL be preserved across delegation boundaries.
Normative Requirement	Governance continuity SHALL be preserved across delegation boundaries.
Conformance Level	L2 — Ordered Governance Mediation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance continuity SHALL be preserved across delegation boundaries.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.45 CR-045 - Governance attribution SHALL remain consistent and unambiguous.

Field	Finding
Requirement Identifier	CR-045
Requirement Name	Governance attribution SHALL remain consistent and unambiguous.
Normative Requirement	Governance attribution SHALL remain consistent and unambiguous.
Conformance Level	L1 — Schema & Envelope Validation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Governance attribution SHALL remain consistent and unambiguous.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.46 CR-046 - Governance context SHALL NOT supersede canonical governance reality.

Field	Finding
Requirement Identifier	CR-046
Requirement Name	Governance context SHALL NOT supersede canonical governance reality.
Normative Requirement	Governance context SHALL NOT supersede canonical governance reality.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance context SHALL NOT supersede canonical governance reality.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.47 CR-047 - Governance provenance SHALL remain continuous across lifecycle transitions.

Field	Finding
Requirement Identifier	CR-047
Requirement Name	Governance provenance SHALL remain continuous across lifecycle transitions.
Normative Requirement	Governance provenance SHALL remain continuous across lifecycle transitions.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance provenance SHALL remain continuous across lifecycle transitions.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.48 CR-048 - Commit decisions SHALL require authoritative governance state.

Field	Finding
Requirement Identifier	CR-048
Requirement Name	Commit decisions SHALL require authoritative governance state.
Normative Requirement	Commit decisions SHALL require authoritative governance state.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Commit decisions SHALL require authoritative governance state.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.49 CR-049 - Governance evaluation SHALL use sufficiently current canonical state.

Field	Finding
Requirement Identifier	CR-049
Requirement Name	Governance evaluation SHALL use sufficiently current canonical state.
Normative Requirement	Governance evaluation SHALL use sufficiently current canonical state.
Conformance Level	L3 — Deterministic Governance
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance evaluation SHALL use sufficiently current canonical state.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The strongest evidence is the commit implementation and the documented stale-authorization scenario. The commit path validates token metadata and lifecycle status, then applies the effect without re-resolving

current inventory or other authoritative state. The pytest suite confirms that a second stale inventory authorization can still commit.

Architectural Interpretation

Architecturally, this is the key distinction between provenance-rich proposal-time authorization and commit-bound AGCP admissibility. The target uses authorization tokens as the execution gate but does not make current canonical state the binding authority at commit.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.50 CR-050 - Governance evaluation SHALL resolve a single authoritative state.

Field	Finding
Requirement Identifier	CR-050
Requirement Name	Governance evaluation SHALL resolve a single authoritative state.
Normative Requirement	Governance evaluation SHALL resolve a single authoritative state.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evaluation SHALL resolve a single authoritative state.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.51 CR-051 - Canonical state SHALL take precedence over non-authoritative observations.

Field	Finding
Requirement Identifier	CR-051
Requirement Name	Canonical state SHALL take precedence over non-authoritative observations.
Normative Requirement	Canonical state SHALL take precedence over non-authoritative observations.
Conformance Level	L3 — Deterministic Governance
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Unknown

Evidence

Type	Location	Rationale
repository_location	acme_supply_ai_execution_governance_architecture	No directly observable or artifact-level evidence was found for this AGCP requirement in the synthetic target package.

Summary

Available evidence was insufficient to assess this requirement directly: Canonical state SHALL take precedence over non-authoritative observations.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.52 CR-052 - Canonical-state integrity SHALL be verifiable and replayable.

Field	Finding
Requirement Identifier	CR-052
Requirement Name	Canonical-state integrity SHALL be verifiable and replayable.
Normative Requirement	Canonical-state integrity SHALL be verifiable and replayable.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Canonical-state integrity SHALL be verifiable and replayable.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.53 CR-053 - Inadmissible actions SHALL be structurally refused.

Field	Finding
Requirement Identifier	CR-053
Requirement Name	Inadmissible actions SHALL be structurally refused.
Normative Requirement	Inadmissible actions SHALL be structurally refused.
Conformance Level	L2 — Ordered Governance Mediation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Inadmissible actions SHALL be structurally refused.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.54 CR-054 - Evidence insufficiency SHALL prevent authorization.

Field	Finding
Requirement Identifier	CR-054
Requirement Name	Evidence insufficiency SHALL prevent authorization.
Normative Requirement	Evidence insufficiency SHALL prevent authorization.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Evidence insufficiency SHALL prevent authorization.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.55 CR-055 - Governance conflicts SHALL prevent operational realization.

Field	Finding
Requirement Identifier	CR-055
Requirement Name	Governance conflicts SHALL prevent operational realization.
Normative Requirement	Governance conflicts SHALL prevent operational realization.
Conformance Level	L3 — Deterministic Governance
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance conflicts SHALL prevent operational realization.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The source evidence is negative evidence: the package intentionally omits the required behavior, or the tests demonstrate behavior that would be refused by a fully commit-bound AGCP implementation.

Architectural Interpretation

The implementation architecture intentionally stops short of the normative AGCP behavior.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.56 CR-056 - Refusals SHALL be attributable governance outcomes.

Field	Finding
Requirement Identifier	CR-056
Requirement Name	Refusals SHALL be attributable governance outcomes.
Normative Requirement	Refusals SHALL be attributable governance outcomes.
Conformance Level	L2 — Ordered Governance Mediation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Refusals SHALL be attributable governance outcomes.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.57 CR-057 - Refusals SHALL be reconstructable and replayable.

Field	Finding
Requirement Identifier	CR-057
Requirement Name	Refusals SHALL be reconstructable and replayable.
Normative Requirement	Refusals SHALL be reconstructable and replayable.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Refusals SHALL be reconstructable and replayable.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.58 CR-058 - Escalation decisions SHALL be evidenced.

Field	Finding
Requirement Identifier	CR-058
Requirement Name	Escalation decisions SHALL be evidenced.
Normative Requirement	Escalation decisions SHALL be evidenced.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

Observed evidence directly supports the requirement: Escalation decisions SHALL be evidenced.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.59 CR-059 - Escalation outcomes SHALL integrate into lifecycle progression.

Field	Finding
Requirement Identifier	CR-059
Requirement Name	Escalation outcomes SHALL integrate into lifecycle progression.
Normative Requirement	Escalation outcomes SHALL integrate into lifecycle progression.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

Observed evidence directly supports the requirement: Escalation outcomes SHALL integrate into lifecycle progression.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.60 CR-060 - Escalation outcomes SHALL support negative adjudication.

Field	Finding
Requirement Identifier	CR-060
Requirement Name	Escalation outcomes SHALL support negative adjudication.
Normative Requirement	Escalation outcomes SHALL support negative adjudication.
Conformance Level	L4 — Execution Authorization Control
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Escalation outcomes SHALL support negative adjudication.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Replace simulated approval flags with verifiable approval artifacts, explicit expiration, cancellation, timeout, and negative-adjudication handling.
- Retain approval and escalation evidence as structured governance records.

6.2.61 CR-061 - Deferred governance decisions SHALL honor validity periods.

Field	Finding
Requirement Identifier	CR-061
Requirement Name	Deferred governance decisions SHALL honor validity periods.
Normative Requirement	Deferred governance decisions SHALL honor validity periods.
Conformance Level	L4 — Execution Authorization Control
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The approve path implements PENDING_HITL handling, approval recording, quorum accumulation, invalid signature rejection by a signature_valid flag, and transition to AUTHORIZED after quorum.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Deferred governance decisions SHALL honor validity periods.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Replace simulated approval flags with verifiable approval artifacts, explicit expiration, cancellation, timeout, and negative-adjudication handling.
- Retain approval and escalation evidence as structured governance records.

6.2.62 CR-062 - Governance outcomes SHALL reference governing state.

Field	Finding
Requirement Identifier	CR-062
Requirement Name	Governance outcomes SHALL reference governing state.
Normative Requirement	Governance outcomes SHALL reference governing state.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL reference governing state.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.63 CR-063 - Governance outcomes SHALL identify governing constraints.

Field	Finding
Requirement Identifier	CR-063
Requirement Name	Governance outcomes SHALL identify governing constraints.
Normative Requirement	Governance outcomes SHALL identify governing constraints.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL identify governing constraints.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.64 CR-064 - Governance outcomes SHALL preserve evidence integrity.

Field	Finding
Requirement Identifier	CR-064
Requirement Name	Governance outcomes SHALL preserve evidence integrity.
Normative Requirement	Governance outcomes SHALL preserve evidence integrity.
Conformance Level	L2 — Ordered Governance Mediation
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Governance outcomes SHALL preserve evidence integrity.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.65 CR-065 - Governance outcomes SHALL be attributable to accountable actors.

Field	Finding
Requirement Identifier	CR-065
Requirement Name	Governance outcomes SHALL be attributable to accountable actors.
Normative Requirement	Governance outcomes SHALL be attributable to accountable actors.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL be attributable to accountable actors.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.66 CR-066 - Governance outcomes SHALL support replay verification.

Field	Finding
Requirement Identifier	CR-066
Requirement Name	Governance outcomes SHALL support replay verification.
Normative Requirement	Governance outcomes SHALL support replay verification.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL support replay verification.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.67 CR-067 - Governance evidence SHALL remain consistent across evaluation and execution.

Field	Finding
Requirement Identifier	CR-067
Requirement Name	Governance evidence SHALL remain consistent across evaluation and execution.
Normative Requirement	Governance evidence SHALL remain consistent across evaluation and execution.
Conformance Level	L3 — Deterministic Governance
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance evidence SHALL remain consistent across evaluation and execution.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The source evidence is negative evidence: the package intentionally omits the required behavior, or the tests demonstrate behavior that would be refused by a fully commit-bound AGCP implementation.

Architectural Interpretation

The implementation architecture intentionally stops short of the normative AGCP behavior.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.68 CR-068 - Commit decisions SHALL remain supportable by evidence.

Field	Finding
Requirement Identifier	CR-068
Requirement Name	Commit decisions SHALL remain supportable by evidence.
Normative Requirement	Commit decisions SHALL remain supportable by evidence.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Commit decisions SHALL remain supportable by evidence.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.69 CR-069 - Evidence continuity SHALL survive multi-agent workflows.

Field	Finding
Requirement Identifier	CR-069
Requirement Name	Evidence continuity SHALL survive multi-agent workflows.
Normative Requirement	Evidence continuity SHALL survive multi-agent workflows.
Conformance Level	L2 — Ordered Governance Mediation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Evidence continuity SHALL survive multi-agent workflows.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

The target is a single synthetic engine, not a distributed multi-agent or cross-implementation interoperability system. The requirement is therefore outside the observable design surface of this package.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.70 CR-070 - Governance continuity SHALL survive agent handoffs.

Field	Finding
Requirement Identifier	CR-070
Requirement Name	Governance continuity SHALL survive agent handoffs.
Normative Requirement	Governance continuity SHALL survive agent handoffs.
Conformance Level	L2 — Ordered Governance Mediation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance continuity SHALL survive agent handoffs.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

The target is a single synthetic engine, not a distributed multi-agent or cross-implementation interoperability system. The requirement is therefore outside the observable design surface of this package.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.71 CR-071 - Agents SHALL preserve required governance context.

Field	Finding
Requirement Identifier	CR-071
Requirement Name	Agents SHALL preserve required governance context.
Normative Requirement	Agents SHALL preserve required governance context.
Conformance Level	L2 — Ordered Governance Mediation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Agents SHALL preserve required governance context.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

The target is a single synthetic engine, not a distributed multi-agent or cross-implementation interoperability system. The requirement is therefore outside the observable design surface of this package.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.72 CR-072 - Governance-domain transitions SHALL remain governed.

Field	Finding
Requirement Identifier	CR-072
Requirement Name	Governance-domain transitions SHALL remain governed.
Normative Requirement	Governance-domain transitions SHALL remain governed.
Conformance Level	L4 — Execution Authorization Control
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance-domain transitions SHALL remain governed.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

The target is a single synthetic engine, not a distributed multi-agent or cross-implementation interoperability system. The requirement is therefore outside the observable design surface of this package.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.73 CR-073 - Governance semantics SHALL be transport-independent.

Field	Finding
Requirement Identifier	CR-073
Requirement Name	Governance semantics SHALL be transport-independent.
Normative Requirement	Governance semantics SHALL be transport-independent.
Conformance Level	L3 — Deterministic Governance
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
repository_location	acme_supply_ai_execution_governance_architecture	No directly executable or artifact-level evidence was found for this AGCP requirement in the synthetic target package.

Summary

Available evidence was insufficient to assess this requirement directly: Governance semantics SHALL be transport-independent.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

No reliable architectural conclusion can be drawn from the available artifacts.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.74 CR-074 - Governance evaluation SHALL be semantically deterministic.

Field	Finding
Requirement Identifier	CR-074
Requirement Name	Governance evaluation SHALL be semantically deterministic.
Normative Requirement	Governance evaluation SHALL be semantically deterministic.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evaluation SHALL be semantically deterministic.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.75 CR-075 - Conformant implementations SHALL produce equivalent governance outcomes.

Field	Finding
Requirement Identifier	CR-075
Requirement Name	Conformant implementations SHALL produce equivalent governance outcomes.
Normative Requirement	Conformant implementations SHALL produce equivalent governance outcomes.
Conformance Level	L3 — Deterministic Governance
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Conformant implementations SHALL produce equivalent governance outcomes.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

The target is a single synthetic engine, not a distributed multi-agent or cross-implementation interoperability system. The requirement is therefore outside the observable design surface of this package.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.76 CR-076 - Governance evaluation SHALL be deterministic.

Field	Finding
Requirement Identifier	CR-076
Requirement Name	Governance evaluation SHALL be deterministic.
Normative Requirement	Governance evaluation SHALL be deterministic.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance evaluation SHALL be deterministic.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.77 CR-077 - Governance evaluation SHALL be node-independent.

Field	Finding
Requirement Identifier	CR-077
Requirement Name	Governance evaluation SHALL be node-independent.
Normative Requirement	Governance evaluation SHALL be node-independent.
Conformance Level	L3 — Deterministic Governance
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance evaluation SHALL be node-independent.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

The target is a single synthetic engine, not a distributed multi-agent or cross-implementation interoperability system. The requirement is therefore outside the observable design surface of this package.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.78 CR-078 - Governance outcomes SHALL be independent of internal agent reasoning variability.

Field	Finding
Requirement Identifier	CR-078
Requirement Name	Governance outcomes SHALL be independent of internal agent reasoning variability.
Normative Requirement	Governance outcomes SHALL be independent of internal agent reasoning variability.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL be independent of internal agent reasoning variability.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.79 CR-079 - Governance SHALL correctly admit admissible actions.

Field	Finding
Requirement Identifier	CR-079
Requirement Name	Governance SHALL correctly admit admissible actions.
Normative Requirement	Governance SHALL correctly admit admissible actions.
Conformance Level	L4 — Execution Authorization Control
Result	Pass
Confidence	High
Determination Basis	fully_observed
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

Observed evidence directly supports the requirement: Governance SHALL correctly admit admissible actions.

Rationale

The source and/or tests demonstrate the required governance behavior using observable implementation evidence. The determination is limited to the synthetic package reviewed and does not imply assurance beyond the executed and inspected evidence.

Evidence Analysis

Evidence consists of source-code behavior and, where available, pytest execution. The observed implementation performs the required evaluation or rejection path directly.

Architectural Interpretation

The implementation aligns with the relevant AGCP architectural concept for the observed scope.

Buyer Implications

This behavior can be considered a demonstrated feature for registry-style feature comparison, subject to the limits of a synthetic, AI-assisted assessment.

Conformance Gap

No conformance gap identified for the observed requirement scope.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Maintain regression coverage for the demonstrated behavior as the governance engine evolves.

6.2.80 CR-080 - Governance SHALL correctly reject inadmissible actions.

Field	Finding
Requirement Identifier	CR-080
Requirement Name	Governance SHALL correctly reject inadmissible actions.
Normative Requirement	Governance SHALL correctly reject inadmissible actions.
Conformance Level	L4 — Execution Authorization Control
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance SHALL correctly reject inadmissible actions.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.81 CR-081 - Governance lifecycle progression SHALL preserve lifecycle integrity.

Field	Finding
Requirement Identifier	CR-081
Requirement Name	Governance lifecycle progression SHALL preserve lifecycle integrity.
Normative Requirement	Governance lifecycle progression SHALL preserve lifecycle integrity.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance lifecycle progression SHALL preserve lifecycle integrity.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.82 CR-082 - Governance state SHALL be derivable from governance records.

Field	Finding
Requirement Identifier	CR-082
Requirement Name	Governance state SHALL be derivable from governance records.
Normative Requirement	Governance state SHALL be derivable from governance records.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance state SHALL be derivable from governance records.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.83 CR-083 - Governance decisions SHALL remain synchronized with authoritative state.

Field	Finding
Requirement Identifier	CR-083
Requirement Name	Governance decisions SHALL remain synchronized with authoritative state.
Normative Requirement	Governance decisions SHALL remain synchronized with authoritative state.
Conformance Level	L3 — Deterministic Governance
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Governance decisions SHALL remain synchronized with authoritative state.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The strongest evidence is the commit implementation and the documented stale-authorization scenario. The commit path validates token metadata and lifecycle status, then applies the effect without re-resolving current inventory or other authoritative state. The pytest suite confirms that a second stale inventory authorization can still commit.

Architectural Interpretation

Architecturally, this is the key distinction between provenance-rich proposal-time authorization and commit-bound AGCP admissibility. The target uses authorization tokens as the execution gate but does not make current canonical state the binding authority at commit.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.84 CR-084 - Admissibility SHALL be commit-bound.

Field	Finding
Requirement Identifier	CR-084
Requirement Name	Admissibility SHALL be commit-bound.
Normative Requirement	Admissibility SHALL be commit-bound.
Conformance Level	L4 — Execution Authorization Control
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Admissibility SHALL be commit-bound.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The strongest evidence is the commit implementation and the documented stale-authorization scenario. The commit path validates token metadata and lifecycle status, then applies the effect without re-resolving current inventory or other authoritative state. The pytest suite confirms that a second stale inventory authorization can still commit.

Architectural Interpretation

Architecturally, this is the key distinction between provenance-rich proposal-time authorization and commit-bound AGCP admissibility. The target uses authorization tokens as the execution gate but does not make current canonical state the binding authority at commit.

Buyer Implications

Buyers should treat this as suitable for illustrating proposal-time governance and authorization-token gating, not as evidence of commit-bound runtime admissibility for stale or conflicting actions.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Core Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.85 CR-085 - Governance decisions SHALL be replayable.

Field	Finding
Requirement Identifier	CR-085
Requirement Name	Governance decisions SHALL be replayable.
Normative Requirement	Governance decisions SHALL be replayable.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance decisions SHALL be replayable.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.86 CR-086 - Governance outcomes SHALL support independent verification.

Field	Finding
Requirement Identifier	CR-086
Requirement Name	Governance outcomes SHALL support independent verification.
Normative Requirement	Governance outcomes SHALL support independent verification.
Conformance Level	L3 — Deterministic Governance
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance outcomes SHALL support independent verification.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.87 CR-087 - Governance SHALL reliably detect inadmissibility.

Field	Finding
Requirement Identifier	CR-087
Requirement Name	Governance SHALL reliably detect inadmissibility.
Normative Requirement	Governance SHALL reliably detect inadmissibility.
Conformance Level	L2 — Ordered Governance Mediation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Governance SHALL reliably detect inadmissibility.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.88 CR-088 - Structural refusal SHALL be enforceable.

Field	Finding
Requirement Identifier	CR-088
Requirement Name	Structural refusal SHALL be enforceable.
Normative Requirement	Structural refusal SHALL be enforceable.
Conformance Level	L4 — Execution Authorization Control
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
source_file	src/acme_governance/engine.py	The governance engine implements proposal submission, schema checks, provenance checks, proposal-time policy evaluation, authorization issuance, hash-linked ledger recording, and token-gated commit behavior.
source_file	src/acme_governance/engine.py	The commit path validates authorization metadata and lifecycle status but intentionally omits current canonical-state re-evaluation and governing-assumption rebinding.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Structural refusal SHALL be enforceable.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.89 CR-089 - Implementations SHALL conform to AGCP governance semantics.

Field	Finding
Requirement Identifier	CR-089
Requirement Name	Implementations SHALL conform to AGCP governance semantics.
Normative Requirement	Implementations SHALL conform to AGCP governance semantics.
Conformance Level	L5 — Multitenant Governance Isolation
Result	Partial
Confidence	Medium
Determination Basis	partial_implementation
Design Relevance	Medium

Evidence

Type	Location	Rationale
repository_location	acme_supply_ai_execution_governance_architecture	No declarative or executable or artifact-level evidence was found for this AGCP requirement in the synthetic target package.

Summary

The target implements a related subset of the required behavior, but does not demonstrate the full AGCP requirement: Implementations SHALL conform to AGCP governance semantics.

Rationale

The implementation contains a meaningful adjacent control, but the observed behavior does not cover every normative condition required by AGCP. The partial result avoids treating related architecture as full conformance.

Evidence Analysis

Evidence demonstrates a related control surface but leaves material AGCP semantics unverified, usually because the system evaluates at proposal time rather than at commit time, uses mutable indexes, or lacks a complete API surface for the requirement.

Architectural Interpretation

The implementation uses a recognizable governance architecture pattern, but the AGCP semantics are narrower or stronger than the behavior demonstrated by the target.

Buyer Implications

This is a buyer-selectable partial capability. Procurement reviewers should confirm whether the narrower implementation is sufficient for their risk context before relying on it.

Conformance Gap

The implementation demonstrates related behavior but lacks one or more AGCP-required semantics, verification surfaces, or lifecycle guarantees.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Extend the related control so that it satisfies the complete AGCP requirement, then add retained test evidence.

6.2.90 CR-090 - Governance semantics SHALL be interoperable and semantically equivalent across implementations.

Field	Finding
Requirement Identifier	CR-090
Requirement Name	Governance semantics SHALL be interoperable and semantically equivalent across implementations.
Normative Requirement	Governance semantics SHALL be interoperable and semantically equivalent across implementations.
Conformance Level	L5 — Multitenant Governance Isolation
Result	Not Assessed
Confidence	Medium
Determination Basis	insufficient_evidence
Design Relevance	Outside Observed Scope

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The target architecture describes a single synthetic implementation and does not provide multi-node, cross-implementation, delegated-authority, or full tenant administration APIs needed to verify this requirement directly.

Summary

Available evidence was insufficient to assess this requirement directly: Governance semantics SHALL be interoperable and semantically equivalent across implementations.

Rationale

The repository does not contain sufficient observable behavior, test evidence, or artifacts to determine whether the requirement is satisfied.

Evidence Analysis

The package does not include enough observable artifacts to evaluate the requirement without inference.

Architectural Interpretation

The target is a single synthetic engine, not a distributed multi-agent or cross-implementation interoperability system. The requirement is therefore outside the observable design surface of this package.

Buyer Implications

This requirement should not be used as a procurement claim without additional evidence or verified assessment activity.

Conformance Gap

Evidence was insufficient to determine conformance.

Scope Interpretation

Outside Observed Scope

Potential Expansion Approaches

- Provide executable evidence, interface documentation, or retained test outputs sufficient to evaluate the requirement directly.

6.2.91 CR-091 - A governance object SHALL enter DEGRADED state when one or more governance assumptions, evidence artifacts, contextual dependencies, authorization conditions, or canonical-state dependencies required for continued admissibility can no longer be verified.

Field	Finding
Requirement Identifier	CR-091
Requirement Name	A governance object SHALL enter DEGRADED state when one or more governance assumptions, evidence artifacts, contextual dependencies, authorization conditions, or canonical-state dependencies required for continued admissibility can no longer be verified.
Normative Requirement	A governance object SHALL enter DEGRADED state when one or more governance assumptions, evidence artifacts, contextual dependencies, authorization conditions, or canonical-state dependencies required for continued admissibility can no longer be verified.
Conformance Level	L2 — Ordered Governance Mediation
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: A governance object SHALL enter DEGRADED state when one or more governance assumptions, evidence artifacts, contextual dependencies, authorization conditions, or canonical-state dependencies required for continued admissibility can no longer be verified.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The source evidence is negative evidence: the package intentionally omits the required behavior, or the tests demonstrate behavior that would be refused by a fully commit-bound AGCP implementation.

Architectural Interpretation

The implementation architecture intentionally stops short of the normative AGCP behavior.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.92 CR-092 - DEGRADED SHALL be a non-terminal lifecycle state.

Field	Finding
Requirement Identifier	CR-092
Requirement Name	DEGRADED SHALL be a non-terminal lifecycle state.
Normative Requirement	DEGRADED SHALL be a non-terminal lifecycle state.
Conformance Level	L2 — Ordered Governance Mediation
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: DEGRADED SHALL be a non-terminal lifecycle state.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The source evidence is negative evidence: the package intentionally omits the required behavior, or the tests demonstrate behavior that would be refused by a fully commit-bound AGCP implementation.

Architectural Interpretation

The implementation architecture intentionally stops short of the normative AGCP behavior.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

6.2.93 CR-093 - Objects in DEGRADED state SHALL require re-evaluation prior to authorization retention or execution.

Field	Finding
Requirement Identifier	CR-093
Requirement Name	Objects in DEGRADED state SHALL require re-evaluation prior to authorization retention or execution.
Normative Requirement	Objects in DEGRADED state SHALL require re-evaluation prior to authorization retention or execution.
Conformance Level	L4 — Execution Authorization Control
Result	Fail
Confidence	High
Determination Basis	implementation_gap
Design Relevance	High

Evidence

Type	Location	Rationale
specification	spec/architecture.md	The architecture documentation explicitly states that the execution gateway does not re-run policy, re-resolve canonical state, re-check governing assumptions, or re-bind target, resource, policy, evidence, and authorization at commit.

Summary

Observable source evidence shows the required behavior is absent or intentionally not implemented: Objects in DEGRADED state SHALL require re-evaluation prior to authorization retention or execution.

Rationale

The inspected implementation either explicitly omits the required behavior or demonstrates a behavior incompatible with the AGCP requirement. This is treated as a conformance gap rather than an architectural criticism of the synthetic target.

Evidence Analysis

The source evidence is negative evidence: the package intentionally omits the required behavior, or the tests demonstrate behavior that would be refused by a fully commit-bound AGCP implementation.

Architectural Interpretation

The implementation architecture intentionally stops short of the normative AGCP behavior.

Buyer Implications

This requirement should not be claimed as satisfied. If needed for a buyer environment, it becomes a potential expansion area rather than an existing capability.

Conformance Gap

Required AGCP behavior is absent or contradicted by observed implementation behavior.

Scope Interpretation

Supporting Scope

Potential Expansion Approaches

- Add commit-bound canonical-state re-resolution and assumption rebinding immediately before execution.
- Represent degraded, expired, superseded, refused, and executed states as derived lifecycle outcomes from governance records.
- Add tests that prove stale authorizations are refused after canonical state, evidence, policy, or authorization assumptions change.

7 Conformance Level Assessment

7.1 Level 1

Field	Finding
Result	Partially Supported
Summary	Level 1 - Schema and Envelope Validation: 6 Pass, 4 Partial, 0 Fail, 1 Not Assessed across 11 mapped requirements.
Rationale	The level result is derived from the requirement findings in the canonical assessment object. Partial and failed requirements are preserved rather than converted into broader conformance claims.

Blocking Gaps

- Open Partial, Fail, or Not Assessed requirement findings remain at this level.

Potential Expansion Approaches

- Close failed and partial requirement findings with implementation evidence and retained test execution before claiming full level support.

7.2 Level 2

Field	Finding
Result	Partially Supported
Summary	Level 2 - Ordered Governance Mediation: 7 Pass, 11 Partial, 2 Fail, 4 Not Assessed across 24 mapped requirements.
Rationale	The level result is derived from the requirement findings in the canonical assessment object. Partial and failed requirements are preserved rather than converted into broader conformance claims.

Blocking Gaps

- Open Partial, Fail, or Not Assessed requirement findings remain at this level.

Potential Expansion Approaches

- Close failed and partial requirement findings with implementation evidence and retained test execution before claiming full level support.

7.3 Level 3

Field	Finding
Result	Partially Supported
Summary	Level 3 - Deterministic Governance: 2 Pass, 11 Partial, 4 Fail, 5 Not Assessed across 22 mapped requirements.
Rationale	The level result is derived from the requirement findings in the canonical assessment object. Partial and failed requirements are preserved rather than converted into broader conformance claims.

Blocking Gaps

- Open Partial, Fail, or Not Assessed requirement findings remain at this level.

Potential Expansion Approaches

- Close failed and partial requirement findings with implementation evidence and retained test execution before claiming full level support.

7.4 Level 4

Field	Finding
Result	Partially Supported
Summary	Level 4 - Execution Authorization Control: 10 Pass, 8 Partial, 10 Fail, 1 Not Assessed across 29 mapped requirements.
Rationale	The level result is derived from the requirement findings in the canonical assessment object. Partial and failed requirements are preserved rather than converted into broader conformance claims.

Blocking Gaps

- Open Partial, Fail, or Not Assessed requirement findings remain at this level.

Potential Expansion Approaches

- Close failed and partial requirement findings with implementation evidence and retained test execution before claiming full level support.

7.5 Level 5

Field	Finding
Result	Partially Supported
Summary	Level 5 - Multitenant Governance Isolation: 0 Pass, 2 Partial, 0 Fail, 5 Not Assessed across 7 mapped requirements.
Rationale	The level result is derived from the requirement findings in the canonical assessment object. Partial and failed requirements are preserved rather than converted into broader conformance claims.

Blocking Gaps

- Open Partial, Fail, or Not Assessed requirement findings remain at this level.

Potential Expansion Approaches

- Close failed and partial requirement findings with implementation evidence and retained test execution before claiming full level support.

8 Governance Coverage Analysis

Coverage analysis summarizes the capability picture from the canonical assessment object. It is descriptive and scope-aware; it does not override conformance findings.

8.1 Strong Coverage

- **Governance Evidence:** Verified within Core Scope with High confidence.
- **Governance Auditability:** Verified within Core Scope with High confidence.

8.2 Partial Coverage

- **Runtime Governance:** Partial coverage within Core Scope with High confidence.
- **Human Authorization Controls:** Partial coverage within Supporting Scope with Medium confidence.
- **Deterministic Governance:** Partial coverage within Supporting Scope with Medium confidence.
- **Governance Continuity:** Partial coverage within Supporting Scope with Medium confidence.
- **Governance Degradation Management:** Partial coverage within Deferred with High confidence.
- **Tenant Isolation:** Partial coverage within Supporting Scope with Medium confidence.

8.3 Limited Coverage

- **Multi-Agent Governance:** Not Present within Outside Observed Scope.
- **Delegation Governance:** Not Present within Outside Observed Scope.

8.4 Capabilities Outside Observed Scope

- **Multi-Agent Governance:** Not Present; confidence High.
- **Delegation Governance:** Not Present; confidence High.

8.5 Coverage Observations

Coverage is strongest where the target records proposal, approval, authorization, commit, refusal, and receipt events. Coverage is partial where AGCP requires commit-bound current-state semantics or cross-system behavior.

8.6 Governance Assurance Considerations

The package supports registry-style characterization but does not include the retained evidence, execution environment capture, or full test engineering expected for Verified or Assured Assessment.

8.7 Procurement Interpretation

Use as a feature-selection example or early due-diligence artifact; do not treat as proof of production AGCP conformance.

8.8 Coverage Interpretation

The governance coverage profile is coherent for a proposal-time governance architecture with intentionally absent commit-bound admissibility.

9 Capability Verification

Capability verification is derived from the capability matrix. Verified maps to Eligible; Partial maps to Further Assessment Required; Not Present and Not Assessed map to Not Eligible.

9.1 Capability Verification Findings

9.1.1 Runtime Governance

Field	Finding
Capability Status	Partial
Verification Result	Further Assessment Required
Derivation Basis	Partial capability maps to Further Assessment Required using the Project Instructions derivation model.

9.1.2 Governance Evidence

Field	Finding
Capability Status	Verified
Verification Result	Eligible
Derivation Basis	Verified capability maps to Eligible using the Project Instructions derivation model.

9.1.3 Human Authorization Controls

Field	Finding
Capability Status	Partial
Verification Result	Further Assessment Required
Derivation Basis	Partial capability maps to Further Assessment Required using the Project Instructions derivation model.

9.1.4 Deterministic Governance

Field	Finding
Capability Status	Partial
Verification Result	Further Assessment Required
Derivation Basis	Partial capability maps to Further Assessment Required using the Project Instructions derivation model.

9.1.5 Governance Continuity

Field	Finding
Capability Status	Partial
Verification Result	Further Assessment Required
Derivation Basis	Partial capability maps to Further Assessment Required using the Project Instructions derivation model.

9.1.6 Governance Degradation Management

Field	Finding
Capability Status	Partial
Verification Result	Further Assessment Required
Derivation Basis	Partial capability maps to Further Assessment Required using the Project Instructions derivation model.

9.1.7 Multi Agent Governance

Field	Finding
Capability Status	Not Present
Verification Result	Not Eligible
Derivation Basis	Not Present capability maps to Not Eligible using the Project Instructions derivation model.

9.1.8 Delegation Governance

Field	Finding
Capability Status	Not Present
Verification Result	Not Eligible
Derivation Basis	Not Present capability maps to Not Eligible using the Project Instructions derivation model.

9.1.9 Tenant Isolation

Field	Finding
Capability Status	Partial
Verification Result	Further Assessment Required
Derivation Basis	Partial capability maps to Further Assessment Required using the Project Instructions derivation model.

9.1.10 Governance Auditability

Field	Finding
Capability Status	Verified
Verification Result	Eligible
Derivation Basis	Verified capability maps to Eligible using the Project Instructions derivation model.

10 Procurement Profile

10.1 Registry Use

Field	Finding
Determination	Suitable as illustrative registry characterization
Basis	The package contains observable source evidence and tests demonstrating a mixed governance profile.
Limitations	Synthetic; not verified or assured.
Recommended Use	Use for buyer education, feature comparison, and methodology validation.

10.2 Operational Reliance

Field	Finding
Determination	Not sufficient for high-assurance operational reliance
Basis	Commit-bound re-evaluation and canonical-state synchronization are absent.
Limitations	Stale authorization can execute after assumptions change.
Recommended Use	Require Verified or Assured Assessment and implementation expansion before relying on AGCP-level commit-bound controls.

11 Registry Determination

11.1 Registry Basis

Field	Value
Registry Identifier	ACME-SUPPLY-AI-EGA-2026-REGISTRY-DEMO
Status	Registry Assessment Complete
Publishable	Illustrative / demo only
Assessment Scope	Synthetic registry assessment based on source review, semantic mapping, and limited pytest execution.
Assessment Findings	Provenance-rich proposal-time governance with partial runtime controls and intentional commit-bound conformance gaps.

11.2 Registry Notes

Registry entry should clearly identify this as an illustrative synthetic assessment and not as a verified product listing.

12 Capability Cards

Card	Eligibility	Basis
Governance Evidence	Eligible	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.
Governance Auditability	Eligible	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.
Runtime Governance	Further Assessment Required	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.
Human Authorization Controls	Further Assessment Required	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.
Deterministic Governance	Further Assessment Required	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.
Governance Continuity	Further Assessment Required	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.

Card	Eligibility	Basis
Governance Degradation Management	Further Assessment Required	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.
Tenant Isolation	Further Assessment Required	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.
Multi-Agent Governance	Not Eligible	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.
Delegation Governance	Not Eligible	Derived from capability verification and capability matrix using the Project Instructions v2.6 mapping.

13 AGCP Integration Profile

Field	Value
Current Status	Proposal-time governance and token-gated execution gateway with hash-linked audit events.
Recommended Profile	AGCP Commit-Bound Governance Expansion Profile if the owner wished to expand toward stronger AGCP conformance.
Next Milestone	Implement commit-time canonical-state re-resolution and stale-authorization refusal tests.

13.1 Rationale

The most valuable AGCP integration point is the commit boundary, where the target currently validates token metadata but does not re-evaluate governing assumptions.

13.2 Potential Expansion Areas

Change	Priority	Related Requirements	Expected Effect
Commit-bound admissibility adapter	Very High	CR-024; CR-031; CR-032; CR-033; CR-084	Would close the central stale-authorization gap.
Lifecycle state derivation	High	CR-081; CR-082; CR-085; CR-091; CR-092; CR-093	Would improve replayability and lifecycle assurance.

14 Optional Governance Expansion Paths

14.1 Strategic Expansion Paths

14.1.1 Position as proposal-time governance with optional AGCP commit-bound roadmap

Priority: High
Rationale: Accurately preserves the value of the current architecture while avoiding overclaiming.
Approach: Publish capability claims narrowly and reserve commit-bound claims for future verified evidence.

14.2 Technical Expansion Paths

14.2.1 Add commit-bound canonical-state re-evaluation

Priority: Very High
Rationale: This is the central technical gap separating the target from AGCP commit-bound semantics.
Approach: Before applying effects, re-resolve tenant, resource, evidence, policy, and authorization assumptions and refuse stale actions.

14.2.2 Replace simulated HITL signatures with verifiable approval artifacts

Priority: Medium
Rationale: CR-016 requires cryptographic attribution and verifiability of governance approvals.
Approach: Use signed approval tokens bound to proposal, tenant, approver, policy, and expiration metadata.

14.3 Conformance Expansion Paths

14.3.1 Add DEGRADED lifecycle state and re-evaluation path

Priority: High
Rationale: CR-091 through CR-093 require degraded-state semantics for unverifiable assumptions.
Approach: Introduce DEGRADED as a non-terminal state and require re-evaluation before authorization retention or execution.