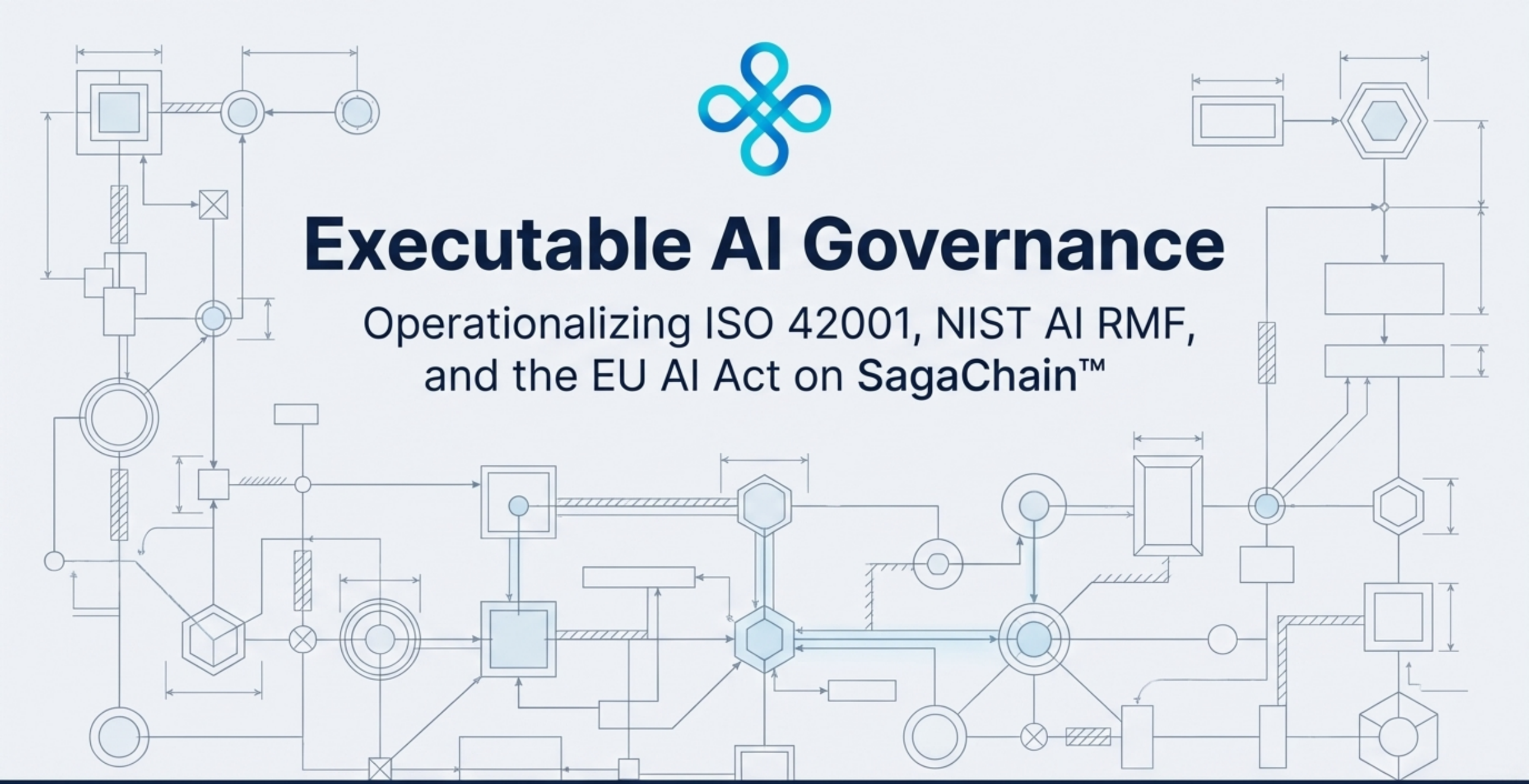


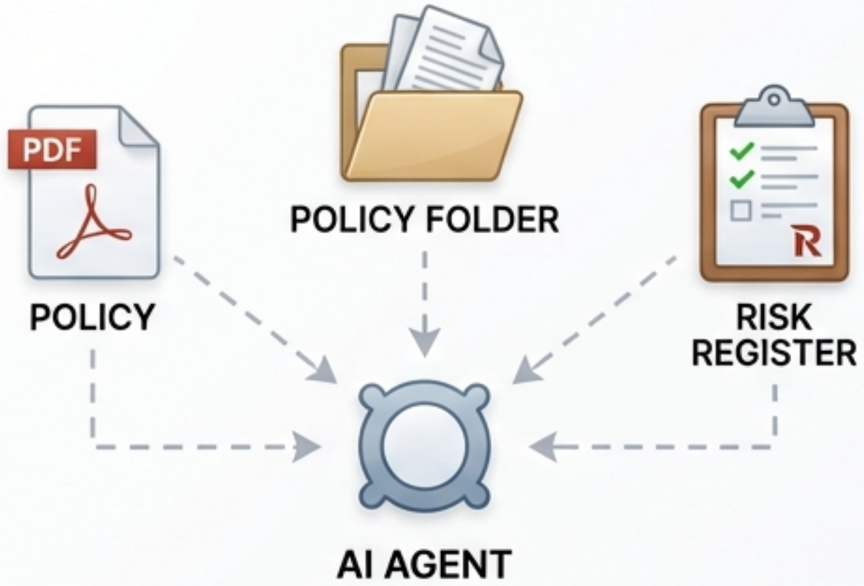
Executable AI Governance

Operationalizing ISO 42001, NIST AI RMF, and the EU AI Act on SagaChain™

Transforming AI compliance from disputable, document-centric narratives into non-bypassable, machine-verifiable infrastructure.

Narrative Governance is Inherently Disputable

Document-Centric



Artifacts exist episodically, **reconstructing posture** rather than anchoring to runtime behavior.

Protocol Limits

Direct protocols lack an **arbitrating entity**. If party logs diverge, there is no computational resolution.

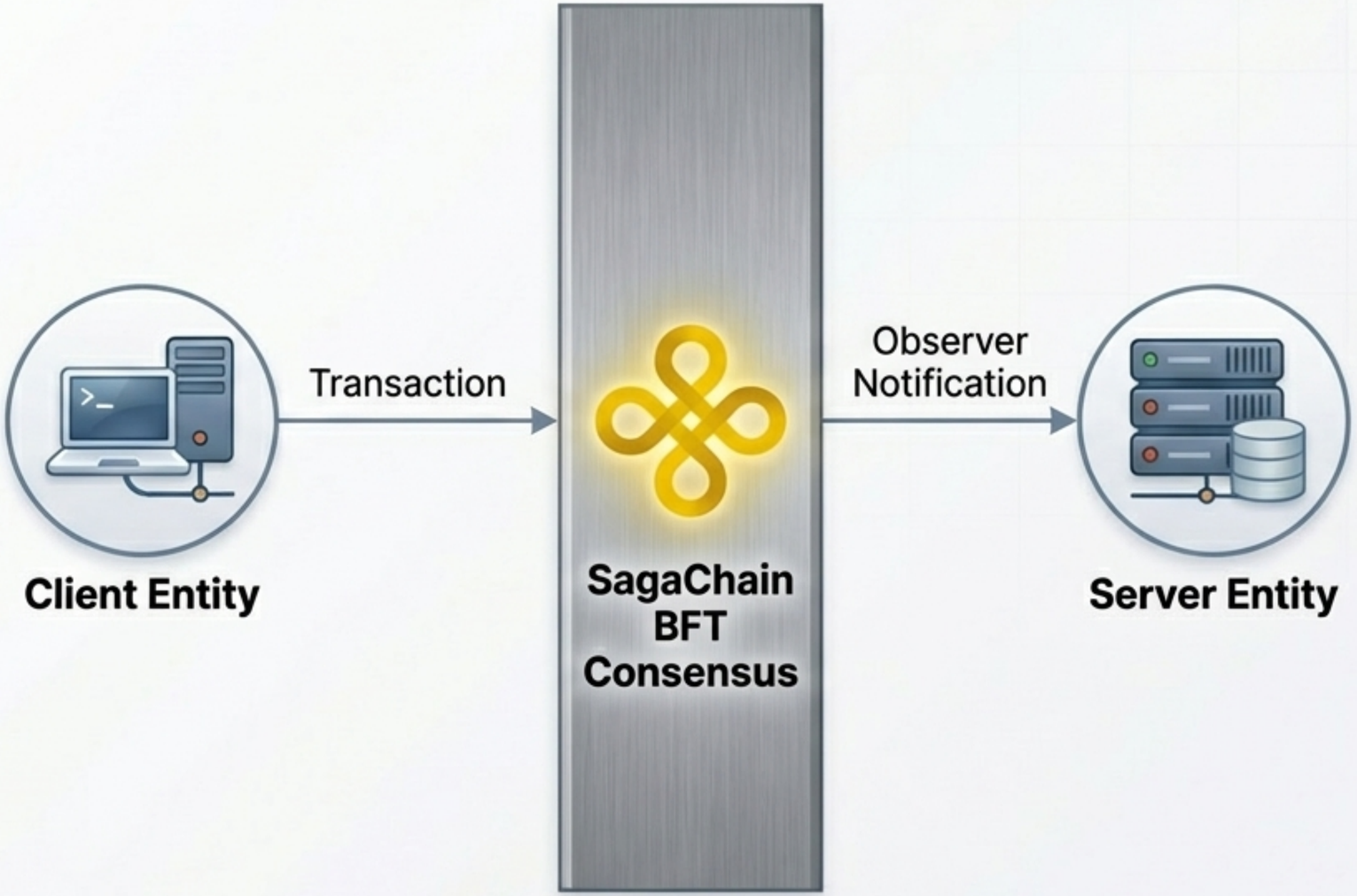
The Architectural Ceiling of Direct AI Protocols

Distributed Governance Requirement	A2A/MCP (Direct)	SagaChain Protocol	Enforcement Mechanism
Authorization	Satisfied	Satisfied + Non-bypassable	Cryptographic TX authorization
Authentication	Satisfied	Satisfied + Non-bypassable	SagaChain TX signing & identity
Account Mgmt	**Disputable**	**Non-disputable**	LOID-anchored provenance objects
Audit Logging	**Disputable**	**Non-disputable**	Immutable consensus blockchain
Accountability	**Disputable**	**Non-disputable**	Observer notification + consensus

Direct client-server models inherently **lack** a single, **non-disputable** source of truth.

The Foundational Fix: Non-Bypassability

1. Interactions are mediated via SagaChain transactions.
2. Transactions require Byzantine Fault Tolerant (BFT) consensus.
3. The append-only log provides a single, indisputable source of truth.



The Executable Architecture Stack

Semantic Governance (SagaStandards): Canonical class definitions, immutable once committed.

Persistent State Anchoring (SagaChain): Immutable lifecycle anchoring via LOIDs and BFT.

Runtime Evaluation (SagaAI): Bounded pre-commit validation of AI functions.

Execution Authority (Institutional): Cryptographic authorization by human actors.

Regulatory Authority: Statutory oversight preserved without displacement.

Structuring Normative Requirements into Deterministic Identity

Canonical Encoding
(Uniform data structures)

Deterministic Identity
(Globally unique LOIDs)
(Content-derived naming)

Referential Binding
(Connecting identity to context)

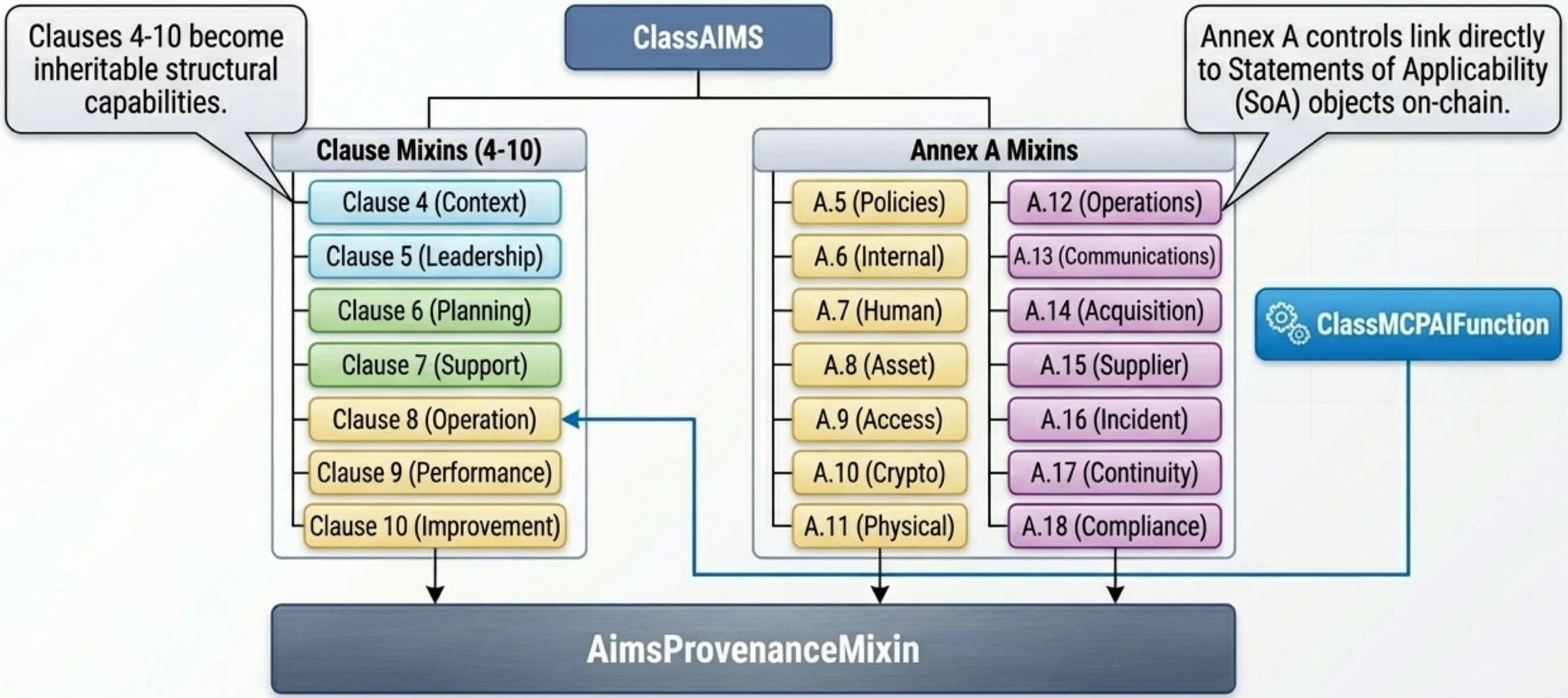
Pre-Commit Validation
(Evaluating structure prior to state mutation)
(Ensuring compliance before change)

Authority Preservation
(Maintaining institutional control)

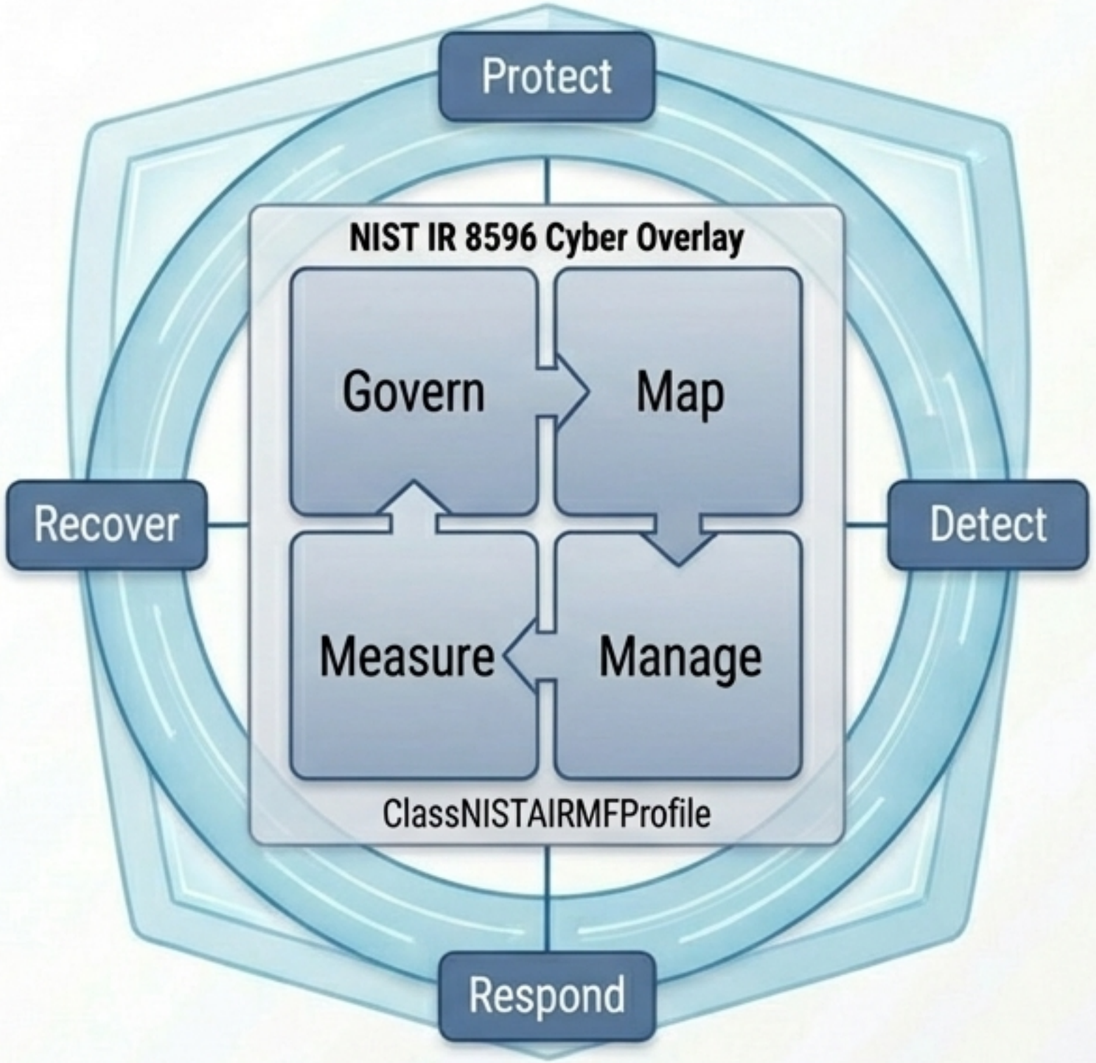
Non-Bypassability
(The immutable consensus boundary)
(Enforced via BFT consensus)

Executable governance requires both canonical object identity and non-bypassable state anchoring; one without the other remains disputable.

Operationalizing ISO/IEC 42001 (AIMS)



Operationalizing the NIST AI RMF & Cyber Overlay



- Policies, risk maps, and mitigation plans become structured, referenceable objects.

- Cybersecurity priority designations directly trigger enhanced pre-commit validation.

EU AI Act Parity Modeling

EU Articles	SagaChain Structural Implementations
Art 9 (Risk)	Mapped to ClassAIIA and RMF objects.
Art 10 (Data)	Enforced via Annex A.6 control objects.
Art 12 (Logging)	Directly and completely satisfied by SagaChain's append-only consensus record (Non-disputable).
Art 13/14 (Transparency & Oversight)	Encoded into object execution gates requiring cryptographic human quorums.

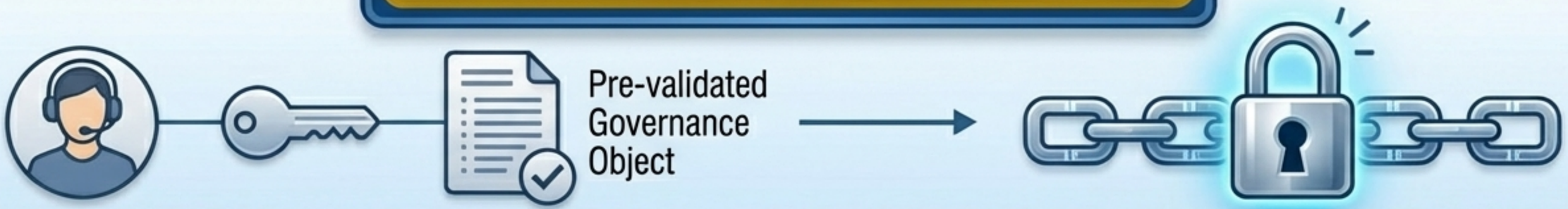
Achieving structural parity without regulatory displacement. Regulators inspect deterministic object lineage instead of reconstructing evidence.

SagaAI Does Not Replace Human Oversight; It Makes It Non-Disputable

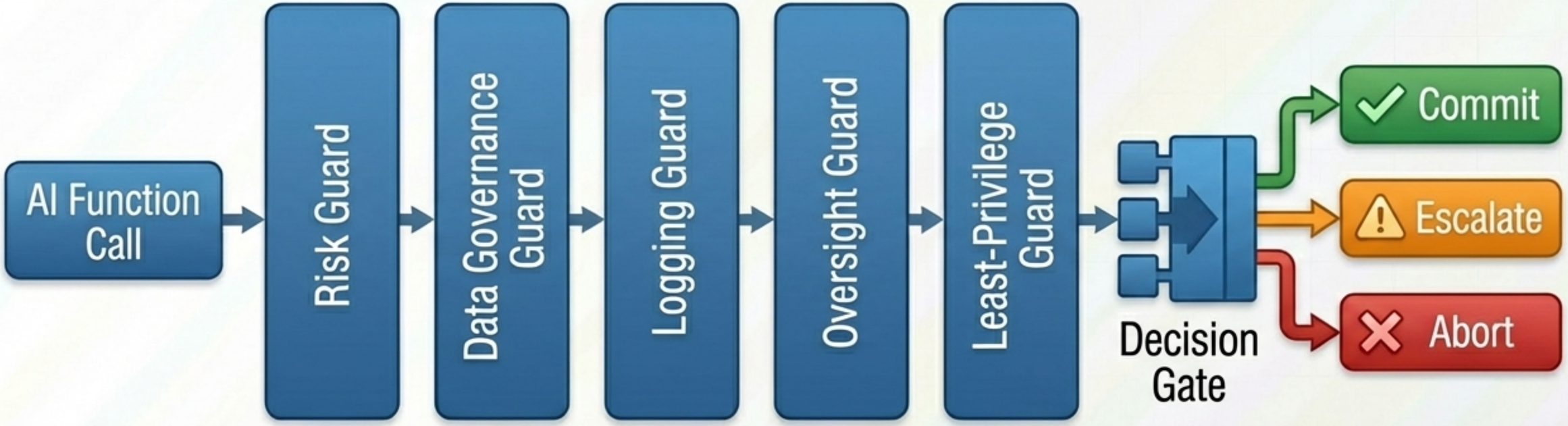
Procedural HITL

Institutional Authorization (Human) **+**
Structural Governance Sufficiency (SagaAI)
= The Commit Boundary.
Neither can be bypassed.

SagaAI Architecture



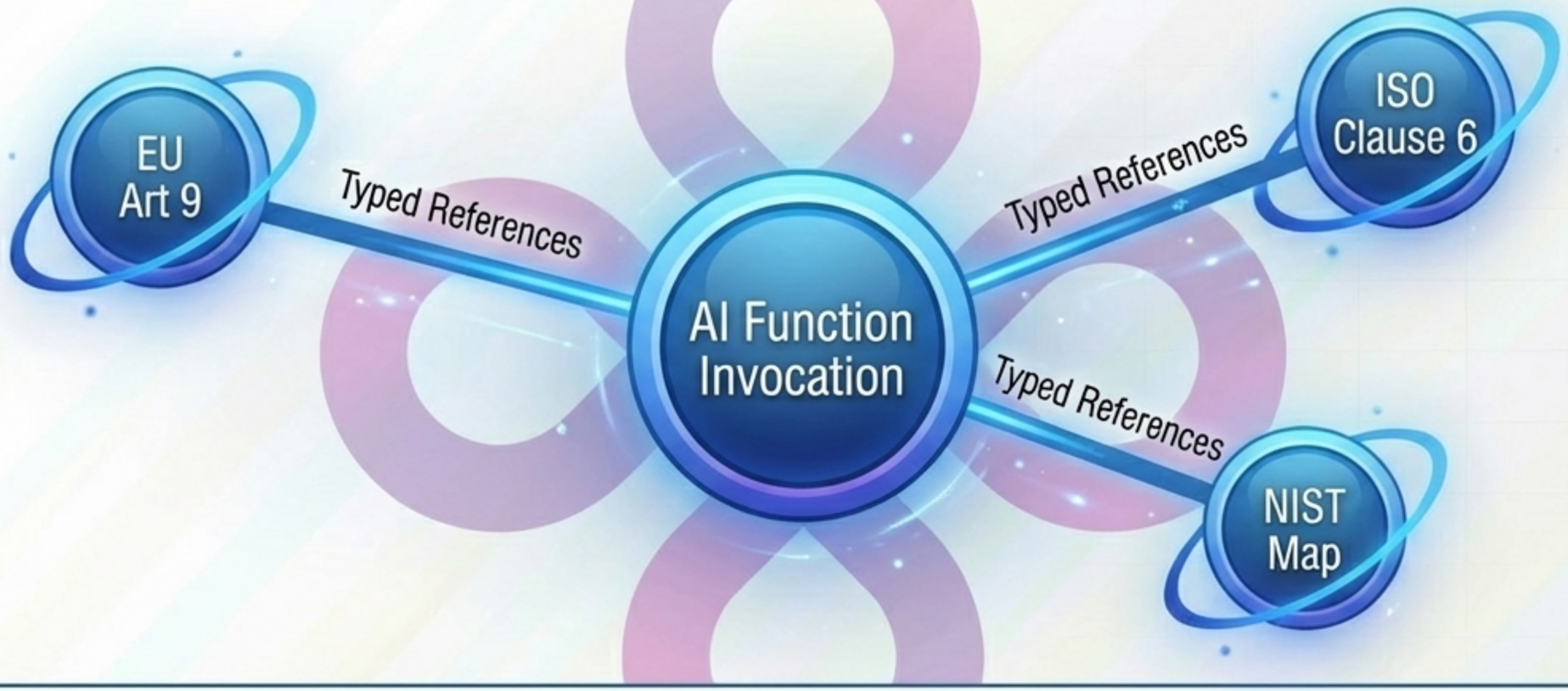
The SagaAI Runtime Guard Architecture



– Evaluates AI function invocations against linked governance objects prior to state mutation.

– All passes, fails, and escalations are immediately recorded as SagaChain transactions.

The Unified Governance Graph



Interoperability without conflation. If a requirement spans NIST and the EU AI Act, both can seamlessly reference the same immutable, LOID-anchored risk object. No dangling references.

Mechanized Governance Invariants (Formal Proofs)

Verified via TLC Model Checker

No Dangling References

Cannot commit an object pointing to a missing record.

Type Completeness

Cross-framework bindings are definitively satisfied before commit.

Guard Non-Bypassability

Every commit requires a cryptographic guard certificate + SagaChain Tx.

Version Evolution Safety

Schema updates cannot retroactively invalidate historical audit states.

Stakeholder Impact: From Document Validation to Object Lineage

Enterprise Operators

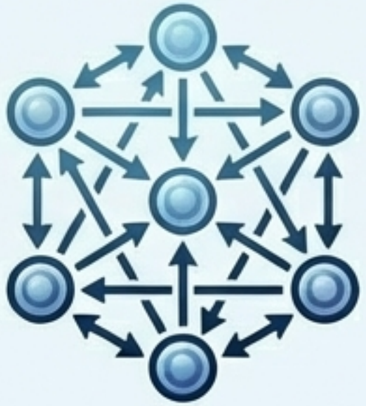
Governance is structurally integrated into workflows. Operational disputes are computationally eliminated.

Regulators

Evidentiary reconstruction is replaced by deterministic, instantaneous object lineage inspection.

Certifiers

Audit integrity is guaranteed; operational state cannot differ from the certified state.



Platforms (A2A/MCP)

Multi-agent interactions become fully auditable without requiring direct trust between agents.

The Epistemic Shift in AI Oversight

- Governance transitions from episodic and supervisory to continuous and infrastructural.
- The 5 A's are elevated from partially satisfied to mathematically guaranteed.
- Institutional actors retain execution authority. Regulators retain interpretive authority. SagaChain secures the non-bypassable substrate.