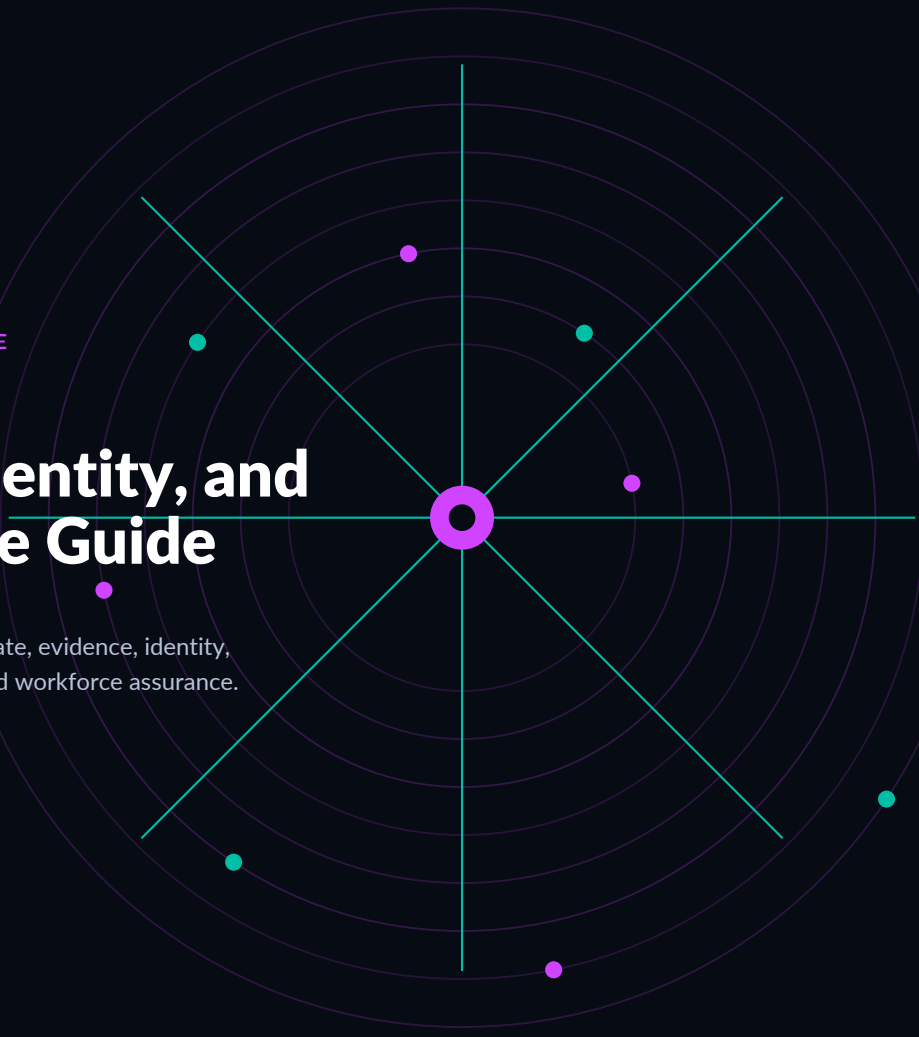
M MYTHOS SYSTEMS

ENGINEERING STANDARDS LIBRARY / ENGINEERING GUIDE

# Knowledge, Data, Identity, and Learning Governance Guide

A permanent governance guide for source authority, state, evidence, identity, authorization, persistent memory, adaptive learning, and workforce assurance.




**PERMANENT DOCUMENT ID**
MYTHOS-GUIDE-KDIL-0001

**PUBLICATION**
Engineering Guide

**STATUS**
Candidate Guide

# Contents

# Executive operating doctrine

Knowledge, data, identity, and learning form the durable substrate around AI. Grounded decisions require authoritative sources, controlled state, explicit identity, verifiable evidence, user-governed memory, and measurable human capability.

# Standards map

| ID | PUBLICATION | CRITERIA |
|---|---|---|
| MYTHOS-KNW-0001 | RAG, Grounding & Source Authority Standard<br>Defines retrieval-augmented generation, grounding, citation, source authority, freshness, conflict handling, provenance, and evidence requirements for knowledge-backed AI systems. | 12 |
| MYTHOS-KNW-0002 | Persona, Avatar & Persistent Memory Architecture Standard<br>Establishes architecture and governance for persistent persona, embodied presence, user-controlled memory, continuity, provenance, privacy, and lifecycle management. | 12 |
| MYTHOS-DAT-0001 | Vector Database & Local-First Sync Architecture Standard<br>Defines vector retrieval and local-first synchronization architecture, including indexing, embeddings, consistency, conflict resolution, offline operation, provenance, and lifecycle control. | 12 |
| MYTHOS-DAT-0002 | AI & Agent Observability Semantic Conventions (OpenTelemetry) Standard<br>Establishes semantic conventions and operational requirements for observing models, agents, tools, retrieval, memory, costs, safety events, and end-to-end AI execution traces. | 11 |
| MYTHOS-DAT-0003 | Data Sovereignty, Privacy Preservation, & Egress Control Standard<br>Defines data sovereignty, privacy preservation, residency, classification, egress control, minimization, policy enforcement, and accountable cross-boundary processing. | 14 |
| MYTHOS-DAT-0004 | Event Sourcing, CQRS, & Durable State Machine Standard<br>Establishes event-sourcing, CQRS, durable state-machine, replay, idempotency, consistency, migration, and evidence requirements for authoritative state systems. | 12 |
| MYTHOS-DAT-0005 | Tamper-Evident Hash-Chained Ledgers & Evidence Bundle Standard<br>Defines tamper-evident ledgers and evidence bundles for consequential system actions, including hash chaining, signatures, provenance, retention, verification, and disclosure boundaries. | 12 |
| MYTHOS-ID-0001 | Workload, Agent & Human Identity Standard<br>Defines identity architecture for humans, workloads, services, agents, tools, and devices with attestation, federation, lifecycle, delegation, authentication, and audit requirements. | 12 |
| MYTHOS-ID-0002 | Public Key Infrastructure (PKI) & Attribute-Based Access Control (ABAC) Standard<br>Establishes public-key infrastructure and attribute-based access-control requirements for trust anchors, certificate lifecycle, policy decision, authorization context, revocation, and evidence. | 12 |
| MYTHOS-EDU-0001 | Adaptive Learning, Skill Graphs & Cyber Lab Standard<br>Defines adaptive learning, skill graphs, competency evidence, cyber labs, assessment, accessibility, credential portability, safety, and workforce-assurance requirements. | 12 |

# Connected governance chain

| SYSTEM | AUTHORITATIVE QUESTION | CONTROL REQUIREMENT |
|---|---|---|
| Knowledge | What sources support the decision, how authoritative are they, and how fresh are they? | Preserve citations, source snapshots, conflicts, access decisions, and uncertainty. |
| Data and state | What is the authoritative state, who may change it, and how is it recovered? | Use typed state models, durable events, integrity, replay, retention, and reconciliation. |
| Identity | Which human, workload, service, agent, device, or tool is acting? | Authenticate and attest the principal; bind lifecycle, delegation, and revocation. |
| Authorization | What may this principal do to this resource in this context? | Evaluate policy externally and issue narrow, expiring, observable capability. |
| Evidence | How can the decision and resulting state be independently reconstructed? | Retain tamper-evident provenance, approvals, verification, and final disposition. |
| Learning | What capability changed, how was it measured, and what evidence supports the credential? | Use transparent skill models, authentic assessment, accessibility, and revocable credentials. |

# Knowledge authority and grounding

| SOURCE CLASS | TYPICAL AUTHORITY | REQUIRED TREATMENT |
|---|---|---|
| Normative authority | Law, regulation, contract, approved policy, or controlled standard. | Pin exact version, jurisdiction, applicability, owner, and expiration. |
| Primary technical source | Official specification, standard, protocol registry, or product documentation. | Record version and retrieval date; distinguish specification from observed behavior. |
| Operational evidence | Logs, tests, measurements, tickets, state snapshots, and signed records. | Protect integrity, time, identity, collection method, retention, and access. |
| Qualified analysis | Reviewed research, expert assessment, or approved internal analysis. | Record method, assumptions, conflicts, confidence, and review date. |
| Secondary synthesis | Books, articles, summaries, and explanatory material. | Use for context, not as sole support for consequential claims. |
| Untrusted or user-generated | Forums, model output, anonymous material, and uncontrolled uploads. | Isolate, label, validate, and prohibit silent promotion into authoritative memory. |

# Data, state, and evidence architecture

| STATE CONCERN | DESIGN QUESTION | ASSURANCE MECHANISM |
|---|---|---|
| Authority | Which store or event stream is authoritative for each entity and decision? | Explicit source-of-truth ownership and conflict policy. |
| Consistency | What stale, divergent, or partial states are acceptable? | Declared consistency model, version vectors, idempotency, and reconciliation. |
| Durability | What must survive process, host, region, and dependency failure? | Write-ahead or event records, checkpoints, backup, restore, and recovery testing. |
| Privacy and sovereignty | Where may data be stored, processed, embedded, retrieved, or disclosed? | Classification, residency, minimization, egress control, deletion, and legal basis. |
| Integrity | How are unauthorized change and evidence tampering detected? | Signatures, hashes, append-only records, access control, and verification. |
| Lifecycle | When is state corrected, migrated, archived, expired, or destroyed? | Versioned schemas, retention schedules, tombstones, and auditable deletion. |
| Observability | Can operators explain state transitions and diagnose divergence? | Correlated traces, events, metrics, logs, and state snapshots. |

# Identity, delegation, and authorization

| PRINCIPAL | IDENTITY PROOF | AUTHORIZATION POSTURE |
|---|---|---|
| Human | Phishing-resistant authentication, account lifecycle, device and session context. | Role, attribute, risk, purpose, and step-up controls with accountable approval. |
| Workload or service | Workload identity, platform attestation, signed deployment, and runtime context. | Short-lived service capability bound to environment, audience, and resource. |
| Agent | Authenticated runtime instance, mission identity, model and configuration lineage. | Delegated capability restricted by mission, tool, target, budget, and expiration. |
| Tool or extension | Signed publisher identity, package provenance, version, permissions, and trust tier. | Explicit grants, sandbox tier, network and filesystem restrictions, and revocation. |
| Device | Hardware or software identity, posture, ownership, and attestation. | Conditional access based on compliance, location, risk, and intended function. |
| Data subject or persona | Verified account relationship, consent, preferences, and representation constraints. | Purpose limitation, user control, privacy, correction, deletion, and impersonation resistance. |

# Adaptive learning and workforce assurance

| LEARNING ELEMENT | CONTROLLED IMPLEMENTATION | EVIDENCE |
|---|---|---|
| Skill graph | Versioned competencies, prerequisites, proficiency levels, and role mappings. | Approved ontology and change history. |
| Adaptive path | Recommendations based on demonstrated gaps, goals, accessibility, and pace. | Explainable recommendation and learner control. |
| Cyber lab | Isolated, resettable, observable environment with scenario and safety boundaries. | Lab configuration, activity telemetry, and cleanup evidence. |
| Assessment | Authentic task, rubric, anti-cheating controls, and human escalation. | Scored artifact, evaluator identity, method, and confidence. |
| Credential | Portable, verifiable achievement tied to evidence and issuer. | Signed credential, criteria, evidence reference, issue and expiration. |
| Continuous assurance | Revalidation after time, role, technology, or risk change. | Review schedule, reassessment result, remediation, and revocation state. |

# Cross-domain failure and recovery

| FAILURE | IMPACT | CONTROL RESPONSE |
|---|---|---|
| Source-authority inversion | Low-quality or adversarial content becomes trusted knowledge. | Quarantine, compare authority, restore lineage, and invalidate derived memory. |
| Stale grounding | Decision cites an obsolete specification, policy, identity, or state snapshot. | Enforce freshness windows, expiration, revalidation, and conflict display. |
| Identity confusion | Agent, service, person, or device is misattributed. | Deny action, reauthenticate or attest, repair correlation, and review delegated capabilities. |
| Excessive delegation | A principal transfers broader or longer authority than intended. | Revoke grants, narrow policy, require approval, and inspect prior activity. |
| State divergence | Offline, distributed, or cached copies disagree with authority. | Enter reconciliation, preserve conflicting versions, and prevent unsafe promotion. |
| Evidence break | Records cannot prove sequence, identity, integrity, or final state. | Classify result as unassured and restore instrumentation before resuming. |
| Learning manipulation | Assessment, skill graph, or adaptive path is gamed or biased. | Review evidence, recalibrate, require alternate assessment, and provide appeal. |
| Privacy over-retention | Memory, embeddings, traces, or credentials persist beyond purpose. | Delete, revoke, rebuild derived indexes, and document residual copies. |

# Minimum evidence by decision domain

| DECISION DOMAIN | MINIMUM EVIDENCE |
|---|---|
| Grounded answer | Claim-to-source mapping, source authority, freshness, retrieval trace, conflicts, and confidence. |
| State transition | Prior state, command or event, authenticated principal, policy decision, resulting state, and verification. |
| Identity issuance | Proofing method, authenticator or workload attestation, issuer, policy, validity, and revocation path. |
| Authorization | Principal, attributes, resource, action, context, policy version, decision, obligations, and expiration. |
| Memory write | Source, purpose, scope, confidence, sensitivity, owner, expiration, correction, and deletion semantics. |
| Credential award | Competency, rubric, assessment evidence, evaluator, issuer, issue date, validity, and revocation. |
| Data movement | Classification, source, destination, purpose, legal or policy basis, transformation, egress decision, and retention. |
| Exception | Control, rationale, risk, compensating controls, owner, approval, expiration, and review result. |

# Implementation roadmap

| PHASE | FOCUS | EXIT CONDITION |
|---|---|---|
| 1. Authority model | Source classes, ownership, exact versions, freshness, and conflict policy. | Approved authority registry and review cadence. |
| 2. Identity substrate | Human, workload, agent, device, and extension identity with lifecycle and attestation. | End-to-end principal correlation and revocation demonstration. |
| 3. State and evidence | Authoritative models, durable events, integrity, replay, and evidence bundles. | Recovery and reconstruction tests pass. |
| 4. Knowledge and memory | Grounded retrieval, provenance, memory scopes, correction, deletion, and contradiction handling. | Poisoning, stale-source, and privacy tests pass. |
| 5. Learning assurance | Skill graphs, accessible labs, authentic assessments, and verifiable credentials. | Evidence-backed credential issuance and appeal process. |
| 6. Continuous governance | Metrics, incidents, exceptions, audits, source expiration, and revalidation. | Operating owners accept SLOs and review obligations. |

# Assurance conclusion

Knowledge informs decisions; identity establishes the actor; policy constrains authority; data records state; evidence makes outcomes reviewable; learning changes capability under transparent and measurable governance. Weakness in any one layer limits the assurance of the entire system.