ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Cloud Architecture and Compute Standards Portfolio

Permanent standards portfolio for cloud architecture and compute.

PERMANENT DOCUMENT ID

MYTHOS-CLD-PORT-0001

PUBLICATION

Portfolio Edition
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Cloud Architecture and Compute Standards Portfolio

DOCUMENT ID
MYTHOS-CLD-PORT-0001

VERSION
1.0.0-candidate

STATUS
Portfolio Edition

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

0	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy cloud architecture and compute standards portfolio system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

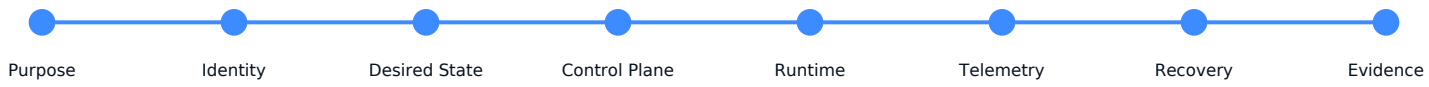
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

MYTHOS-CLD-PORT-0001 / CLOUD ARCHITECTURE

Portfolio Position

Permanent standards portfolio for cloud architecture and compute.

OPERATING POSITION

This portfolio consolidates 11 permanent standards for cloud architecture and compute.

- Use it to establish a shared control vocabulary, implementation sequence, evidence profile, and adoption roadmap.
- Individual standards remain independently identifiable and citable.

MYTHOS-CLD-PORT-0001 / CLOUD ARCHITECTURE

Portfolio Register

MYTHOS-CLD-0001
Multi-Cloud Architecture and Control Plane Standard

MYTHOS-CLD-0002
AWS Architecture, Security, and Automation Standard

MYTHOS-CLD-0003
Microsoft Azure Architecture, Security, and Automation Standard

MYTHOS-CLD-0004
Google Cloud Architecture and Automation Standard

MYTHOS-CLD-0005
Oracle Cloud Infrastructure Architecture and Automation Standard

MYTHOS-CLD-0006
Alibaba Cloud Architecture and Automation Standard

MYTHOS-CLD-0007
Kubernetes, Container Orchestration, and Operator Standard

MYTHOS-CLD-0008
Serverless and Event-Driven Compute Standard

MYTHOS-CLD-0009
Decentralized Physical Infrastructure Networks Standard

MYTHOS-CLD-0010
Private Cloud, Hypervisor, and Bare-Metal Standard

MYTHOS-CLD-0011
Web3 and Decentralized Ledger Architecture Standard

Permanent identities remain independently citable across revision, portfolio assembly, distribution, and archival packaging.

MYTHOS-CLD-PORT-0001 / CLOUD ARCHITECTURE

Control Architecture

OPERATING POSITION

Reasoning proposes; policy authorizes; deterministic systems execute; evidence records.

- State, identity, sources, and learning remain governed throughout the lifecycle.
- High-consequence use requires stronger isolation, approval, reproducibility, and recovery.

MYTHOS-CLD-PORT-0001 / CLOUD ARCHITECTURE

Assurance Model

OPERATING POSITION

Six assurance views: governance, architecture, security, operations, privacy/rights, and human/societal impact.

- Three implementation profiles: Foundational, Advanced, and High Assurance.
- Atomic criteria receive pass, partial, fail, not-applicable, or controlled-exception disposition.

MYTHOS-CLD-PORT-0001 / CLOUD ARCHITECTURE

Adoption Sequence

OPERATING POSITION

Establish ownership and inventory.

- Classify consequence and select profile.
- Create enforceable identity, policy, execution, and data boundaries.
- Evaluate representative workloads and adversarial cases.
- Release gradually with rollback and evidence.
- Operate, reassess, and retire with preserved records.

MYTHOS-CLD-PORT-0001 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Multi-Cloud Architecture and Control Plane Standard

Cross-provider portfolio governance, landing zones, identity, policy, sovereignty, resilience, cost, evidence, and exit.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0001

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Multi-Cloud Architecture and Control Plane Standard

DOCUMENT ID
MYTHOS-CLD-0001

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy multi-cloud architecture and control plane system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

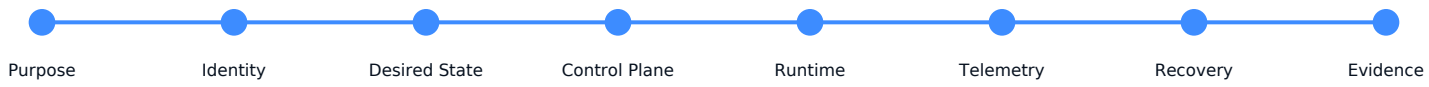
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting multi-cloud architecture and control plane capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for multi-cloud architecture and control plane across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of multi-cloud architecture and control plane capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

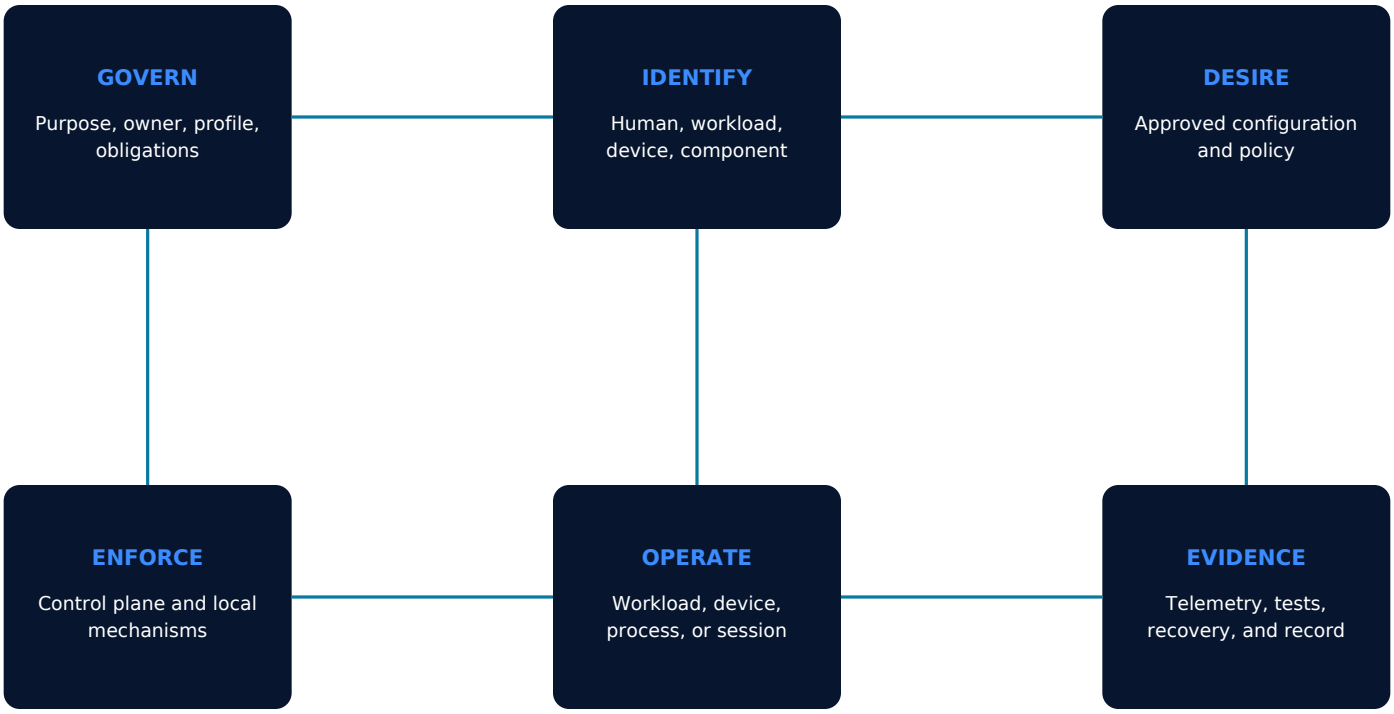
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0001-C01 Cloud Portfolio Strategy and Service Boundary

The organization MUST define, implement, verify, and maintain cloud portfolio strategy and service boundary for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0001-C02 Provider, Region, and Service Approval

The organization MUST define, implement, verify, and maintain provider, region, and service approval for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0001-C03 Organization, Tenancy, and Account Hierarchy

The organization MUST define, implement, verify, and maintain organization, tenancy, and account hierarchy for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0001-C04 Landing Zone and Environment Segmentation

The organization MUST define, implement, verify, and maintain landing zone and environment segmentation for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0001-C05 Federated Identity and Privileged Administration

The organization MUST define, implement, verify, and maintain federated identity and privileged administration for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0001-C06 Cross-Cloud Network and Egress Architecture

The organization MUST define, implement, verify, and maintain cross-cloud network and egress architecture for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0001-C07 Data Classification, Residency, and Sovereignty

The organization MUST define, implement, verify, and maintain data classification, residency, and sovereignty for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0001-C08 Encryption, Key Authority, and Secret Protection

The organization MUST define, implement, verify, and maintain encryption, key authority, and secret protection for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0001-C09 Policy-as-Code and Preventive Guardrails

The organization MUST define, implement, verify, and maintain policy-as-code and preventive guardrails for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0001-C10 Workload Onboarding and Shared-Service Contract

The organization MUST define, implement, verify, and maintain workload onboarding and shared-service contract for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0001-C11 Telemetry, Inventory, and Evidence Normalization

The organization MUST define, implement, verify, and maintain telemetry, inventory, and evidence normalization for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0001-C12 FinOps, Quota, and Capacity Governance

The organization MUST define, implement, verify, and maintain finops, quota, and capacity governance for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0001-C13 Failure-Domain and Provider-Outage Strategy

The organization MUST define, implement, verify, and maintain failure-domain and provider-outage strategy for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0001-C14 Backup, Restoration, and Cyber-Recovery

The organization MUST define, implement, verify, and maintain backup, restoration, and cyber-recovery for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0001-C15 Cloud Incident Response and Escalation

The organization MUST define, implement, verify, and maintain cloud incident response and escalation for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0001-C16 Supplier, Marketplace, and Dependency Governance

The organization MUST define, implement, verify, and maintain supplier, marketplace, and dependency governance for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0001-C17 Portability, Interoperability, and Exit Testing

The organization MUST define, implement, verify, and maintain portability, interoperability, and exit testing for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0001-C18 Conformance Evidence and Reassessment

The organization MUST define, implement, verify, and maintain conformance evidence and reassessment for in-scope multi-cloud architecture and control plane capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0001 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

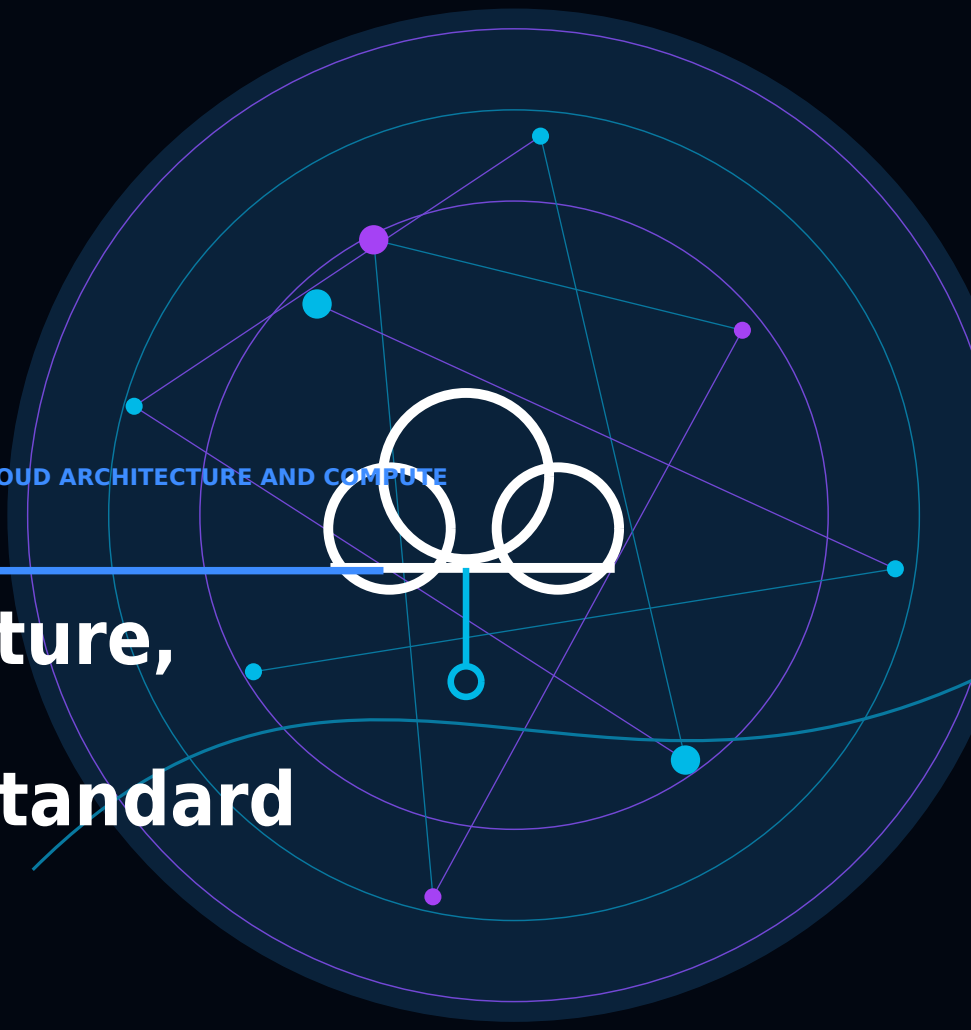
SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0001

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY



ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

AWS Architecture, Security, and Automation Standard

AWS organization design, landing zones, identity, networking, data, automation, resilience, operations, and evidence.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0002

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

AWS Architecture, Security, and Automation Standard

DOCUMENT ID
MYTHOS-CLD-0002

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy AWS cloud architecture system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

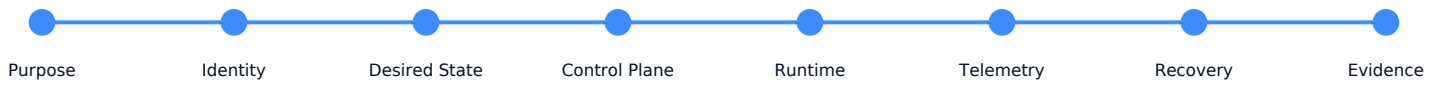
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting AWS cloud architecture capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for AWS cloud architecture across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of AWS cloud architecture capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

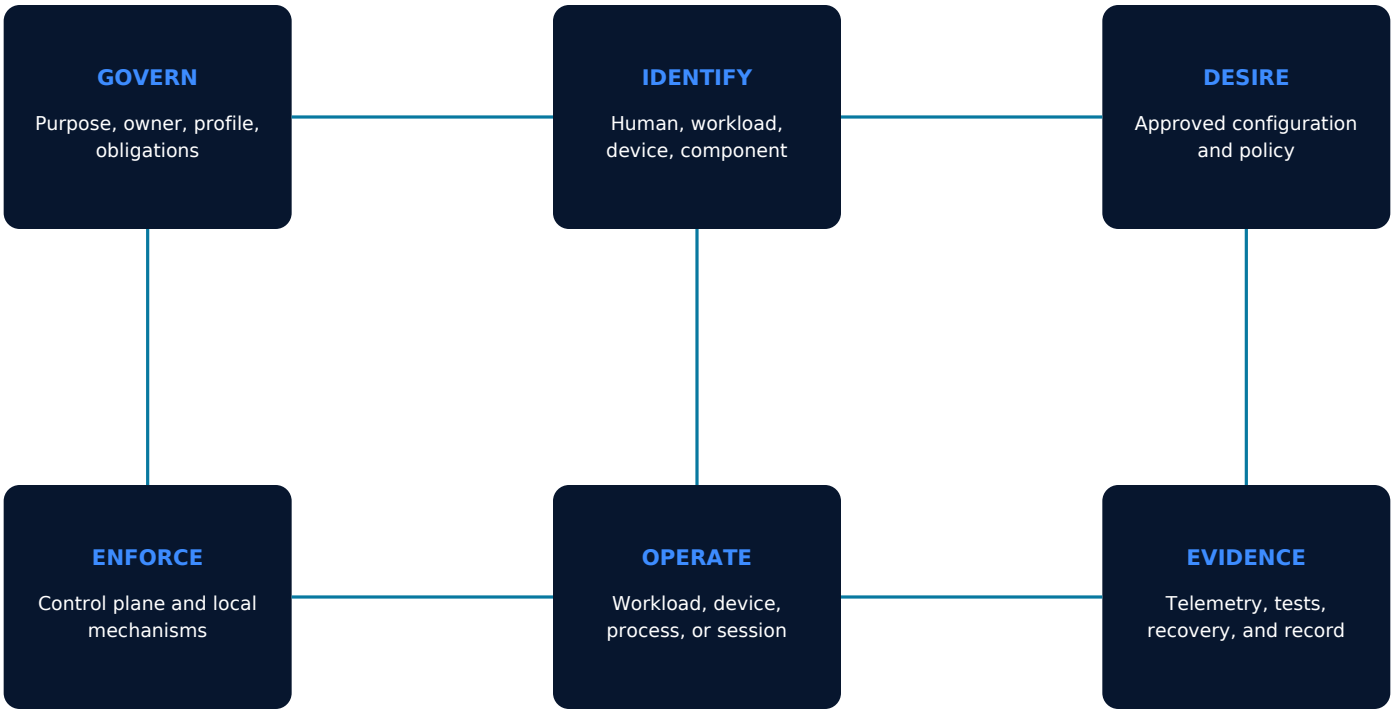
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0002-C01 AWS Tenancy, Organization, and Account Hierarchy

The organization MUST define, implement, verify, and maintain aws tenancy, organization, and account hierarchy for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0002-C02 AWS Landing Zone and Environment Segmentation

The organization MUST define, implement, verify, and maintain aws landing zone and environment segmentation for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0002-C03 AWS Identity Federation and Privileged Administration

The organization MUST define, implement, verify, and maintain aws identity federation and privileged administration for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0002-C04 AWS Resource Policy and Preventive Guardrails

The organization MUST define, implement, verify, and maintain aws resource policy and preventive guardrails for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0002-C05 AWS Network Topology, Ingress, and Egress Control

The organization MUST define, implement, verify, and maintain aws network topology, ingress, and egress control for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0002-C06 AWS Encryption, Key Authority, and Secret Protection

The organization MUST define, implement, verify, and maintain aws encryption, key authority, and secret protection for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0002-C07 AWS Data Classification, Residency, and Service Selection

The organization MUST define, implement, verify, and maintain aws data classification, residency, and service selection for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0002-C08 AWS Workload Identity and Service Authorization

The organization MUST define, implement, verify, and maintain aws workload identity and service authorization for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0002-C09 AWS Declarative Provisioning and Change Control

The organization MUST define, implement, verify, and maintain aws declarative provisioning and change control for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0002-C10 AWS Artifact, Image, and Software Supply-Chain Assurance

The organization MUST define, implement, verify, and maintain aws artifact, image, and software supply-chain assurance for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0002-C11 AWS Logging, Telemetry, and Security Monitoring

The organization MUST define, implement, verify, and maintain aws logging, telemetry, and security monitoring for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0002-C12 AWS Reliability, Availability-Zone, and Region Strategy

The organization MUST define, implement, verify, and maintain aws reliability, availability-zone, and region strategy for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0002-C13 AWS Backup, Restoration, and Cyber-Recovery

The organization MUST define, implement, verify, and maintain aws backup, restoration, and cyber-recovery for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0002-C14 AWS Vulnerability, Configuration, and Drift Management

The organization MUST define, implement, verify, and maintain aws vulnerability, configuration, and drift management for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0002-C15 AWS Cost, Quota, Capacity, and FinOps Governance

The organization MUST define, implement, verify, and maintain aws cost, quota, capacity, and finops governance for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0002-C16 AWS Incident Response and Provider Escalation

The organization MUST define, implement, verify, and maintain aws incident response and provider escalation for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0002-C17 AWS Portability, Exit, and Data Disposition

The organization MUST define, implement, verify, and maintain aws portability, exit, and data disposition for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0002-C18 AWS Evidence Package and Periodic Reassessment

The organization MUST define, implement, verify, and maintain aws evidence package and periodic reassessment for in-scope AWS cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0002 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0002

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Microsoft Azure Architecture, Security, and Automation Standard

Azure tenant and management-group design, Entra identity, policy, networking, data, automation, resilience, and evidence.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0003

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Microsoft Azure Architecture, Security, and Automation Standard

DOCUMENT ID
MYTHOS-CLD-0003

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy Microsoft Azure architecture system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW

Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting Microsoft Azure architecture capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for Microsoft Azure architecture across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of Microsoft Azure architecture capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

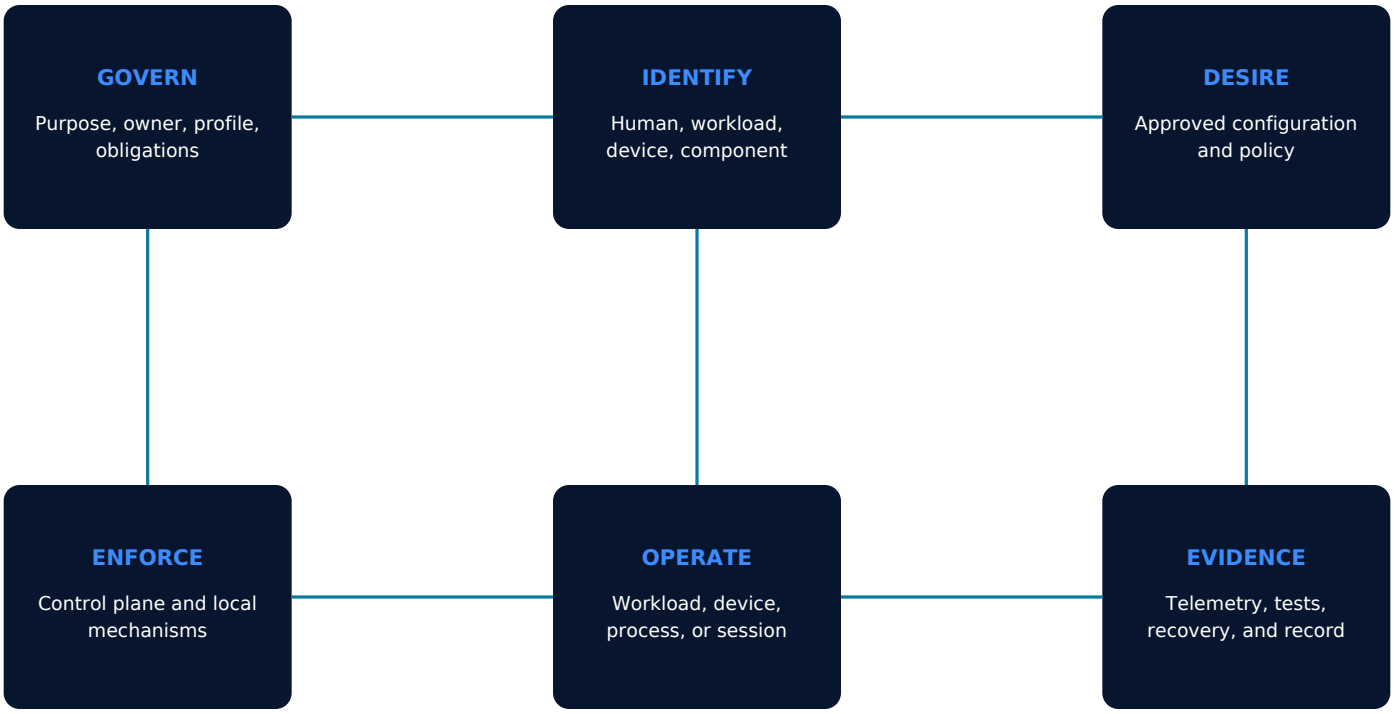
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0003-C01 Microsoft Azure Tenancy, Organization, and Account Hierarchy

The organization MUST define, implement, verify, and maintain microsoft azure tenancy, organization, and account hierarchy for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0003-C02 Microsoft Azure Landing Zone and Environment Segmentation

The organization MUST define, implement, verify, and maintain microsoft azure landing zone and environment segmentation for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0003-C03 Microsoft Azure Identity Federation and Privileged Administration

The organization MUST define, implement, verify, and maintain microsoft azure identity federation and privileged administration for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0003-C04 Microsoft Azure Resource Policy and Preventive Guardrails

The organization MUST define, implement, verify, and maintain microsoft azure resource policy and preventive guardrails for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0003-C05 Microsoft Azure Network Topology, Ingress, and Egress Control

The organization MUST define, implement, verify, and maintain microsoft azure network topology, ingress, and egress control for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0003-C06 Microsoft Azure Encryption, Key Authority, and Secret Protection

The organization MUST define, implement, verify, and maintain microsoft azure encryption, key authority, and secret protection for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0003-C07 Microsoft Azure Data Classification, Residency, and Service Selection

The organization MUST define, implement, verify, and maintain microsoft azure data classification, residency, and service selection for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0003-C08 Microsoft Azure Workload Identity and Service Authorization

The organization MUST define, implement, verify, and maintain microsoft azure workload identity and service authorization for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0003-C09 Microsoft Azure Declarative Provisioning and Change Control

The organization MUST define, implement, verify, and maintain microsoft azure declarative provisioning and change control for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0003-C10 Microsoft Azure Artifact, Image, and Software Supply-Chain Assurance

The organization MUST define, implement, verify, and maintain microsoft azure artifact, image, and software supply-chain assurance for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0003-C11 Microsoft Azure Logging, Telemetry, and Security Monitoring

The organization MUST define, implement, verify, and maintain microsoft azure logging, telemetry, and security monitoring for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0003-C12 Microsoft Azure Reliability, Availability-Zone, and Region Strategy

The organization MUST define, implement, verify, and maintain microsoft azure reliability, availability-zone, and region strategy for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0003-C13 Microsoft Azure Backup, Restoration, and Cyber-Recovery

The organization MUST define, implement, verify, and maintain microsoft azure backup, restoration, and cyber-recovery for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0003-C14 Microsoft Azure Vulnerability, Configuration, and Drift Management

The organization MUST define, implement, verify, and maintain microsoft azure vulnerability, configuration, and drift management for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0003-C15 Microsoft Azure Cost, Quota, Capacity, and FinOps Governance

The organization MUST define, implement, verify, and maintain microsoft azure cost, quota, capacity, and finops governance for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0003-C16 Microsoft Azure Incident Response and Provider Escalation

The organization MUST define, implement, verify, and maintain microsoft azure incident response and provider escalation for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0003-C17 Microsoft Azure Portability, Exit, and Data Disposition

The organization MUST define, implement, verify, and maintain microsoft azure portability, exit, and data disposition for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0003-C18 Microsoft Azure Evidence Package and Periodic Reassessment

The organization MUST define, implement, verify, and maintain microsoft azure evidence package and periodic reassessment for in-scope Microsoft Azure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0003 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0003

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Google Cloud Architecture and Automation Standard

Google Cloud resource hierarchy, identity, policy, network, data, workload, resilience, automation, and evidence.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0004

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Google Cloud Architecture and Automation Standard

DOCUMENT ID
MYTHOS-CLD-0004

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy Google Cloud architecture system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW

Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting Google Cloud architecture capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for Google Cloud architecture across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of Google Cloud architecture capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

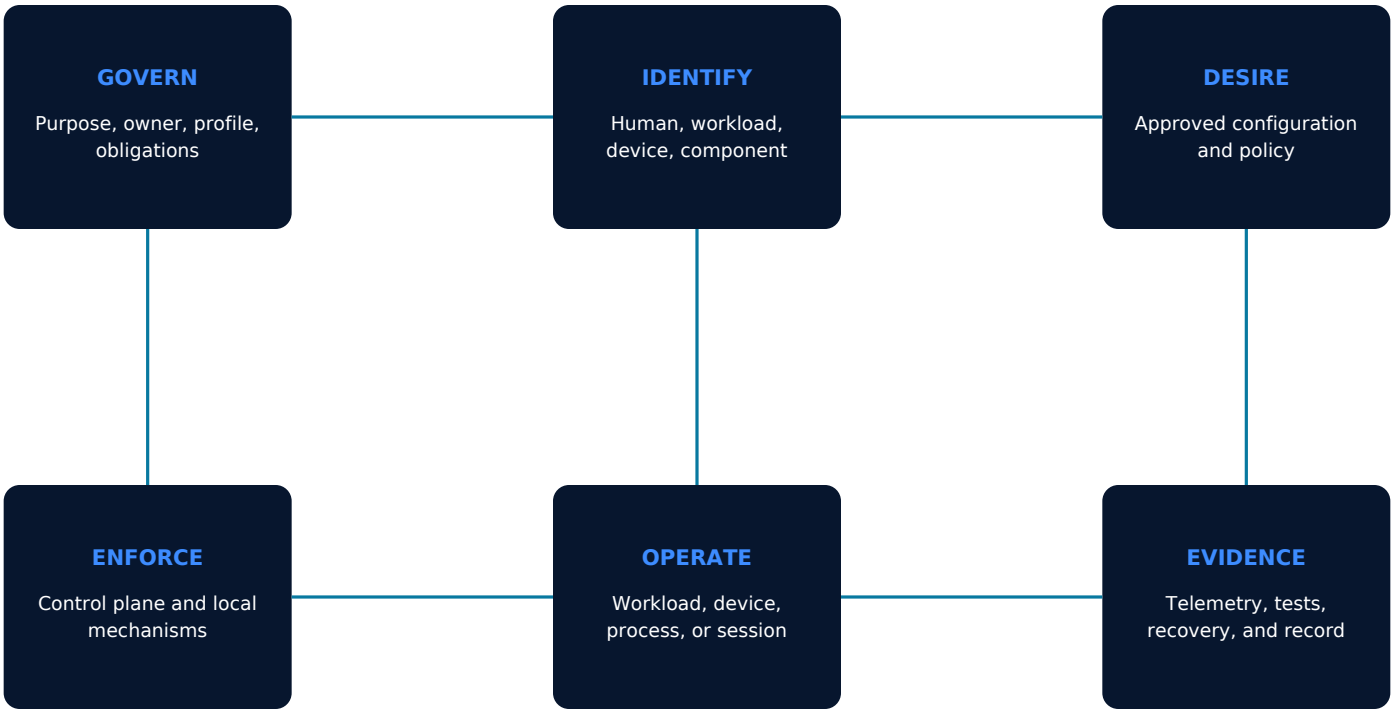
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0004-C01 Google Cloud Tenancy, Organization, and Account Hierarchy

The organization MUST define, implement, verify, and maintain google cloud tenancy, organization, and account hierarchy for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0004-C02 Google Cloud Landing Zone and Environment Segmentation

The organization MUST define, implement, verify, and maintain google cloud landing zone and environment segmentation for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0004-C03 Google Cloud Identity Federation and Privileged Administration

The organization MUST define, implement, verify, and maintain google cloud identity federation and privileged administration for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0004-C04 Google Cloud Resource Policy and Preventive Guardrails

The organization MUST define, implement, verify, and maintain google cloud resource policy and preventive guardrails for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0004-C05 Google Cloud Network Topology, Ingress, and Egress Control

The organization MUST define, implement, verify, and maintain google cloud network topology, ingress, and egress control for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0004-C06 Google Cloud Encryption, Key Authority, and Secret Protection

The organization MUST define, implement, verify, and maintain google cloud encryption, key authority, and secret protection for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0004-C07 Google Cloud Data Classification, Residency, and Service Selection

The organization MUST define, implement, verify, and maintain google cloud data classification, residency, and service selection for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0004-C08 Google Cloud Workload Identity and Service Authorization

The organization MUST define, implement, verify, and maintain google cloud workload identity and service authorization for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0004-C09 Google Cloud Declarative Provisioning and Change Control

The organization MUST define, implement, verify, and maintain google cloud declarative provisioning and change control for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0004-C10 Google Cloud Artifact, Image, and Software Supply-Chain Assurance

The organization MUST define, implement, verify, and maintain google cloud artifact, image, and software supply-chain assurance for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0004-C11 Google Cloud Logging, Telemetry, and Security Monitoring

The organization MUST define, implement, verify, and maintain google cloud logging, telemetry, and security monitoring for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0004-C12 Google Cloud Reliability, Availability-Zone, and Region Strategy

The organization MUST define, implement, verify, and maintain google cloud reliability, availability-zone, and region strategy for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0004-C13 Google Cloud Backup, Restoration, and Cyber-Recovery

The organization MUST define, implement, verify, and maintain google cloud backup, restoration, and cyber-recovery for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0004-C14 Google Cloud Vulnerability, Configuration, and Drift Management

The organization MUST define, implement, verify, and maintain google cloud vulnerability, configuration, and drift management for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0004-C15 Google Cloud Cost, Quota, Capacity, and FinOps Governance

The organization MUST define, implement, verify, and maintain google cloud cost, quota, capacity, and finops governance for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0004-C16 Google Cloud Incident Response and Provider Escalation

The organization MUST define, implement, verify, and maintain google cloud incident response and provider escalation for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0004-C17 Google Cloud Portability, Exit, and Data Disposition

The organization MUST define, implement, verify, and maintain google cloud portability, exit, and data disposition for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0004-C18 Google Cloud Evidence Package and Periodic Reassessment

The organization MUST define, implement, verify, and maintain google cloud evidence package and periodic reassessment for in-scope Google Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0004 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0004

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Oracle Cloud Infrastructure Architecture and Automation Standard

OCI tenancy, compartments, identity domains, network, data, automation, resilience, operations, and evidence.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0005

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Oracle Cloud Infrastructure Architecture and Automation Standard

DOCUMENT ID
MYTHOS-CLD-0005

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy Oracle Cloud Infrastructure architecture system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

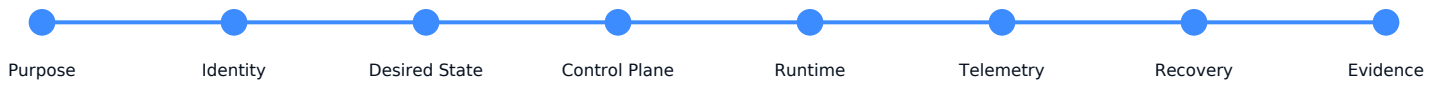
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting Oracle Cloud Infrastructure architecture capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for Oracle Cloud Infrastructure architecture across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of Oracle Cloud Infrastructure architecture capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

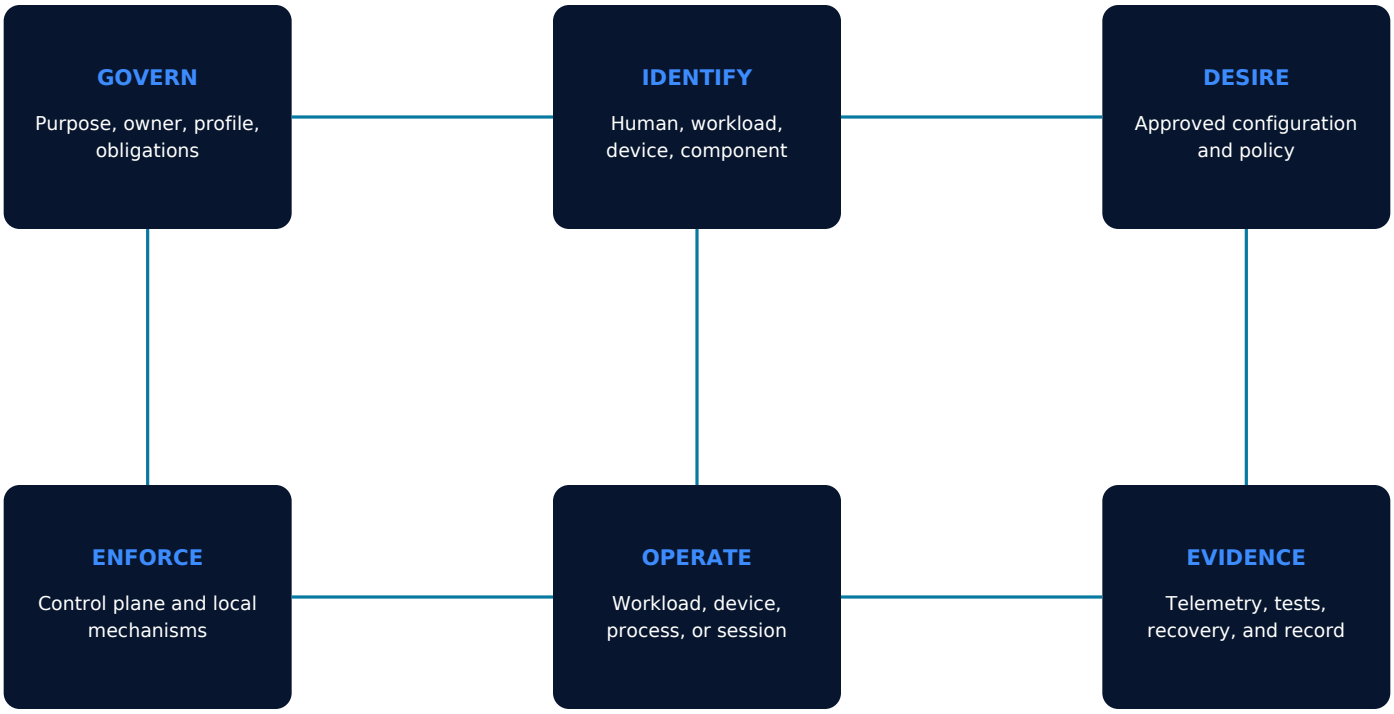
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0005-C01 Oracle Cloud Infrastructure Tenancy, Organization, and Account Hierarchy

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure tenancy, organization, and account hierarchy for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0005-C02 Oracle Cloud Infrastructure Landing Zone and Environment Segmentation

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure landing zone and environment segmentation for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0005-C03 Oracle Cloud Infrastructure Identity Federation and Privileged Administration

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure identity federation and privileged administration for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0005-C04 Oracle Cloud Infrastructure Resource Policy and Preventive Guardrails

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure resource policy and preventive guardrails for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0005-C05 Oracle Cloud Infrastructure Network Topology, Ingress, and Egress Control

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure network topology, ingress, and egress control for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0005-C06 Oracle Cloud Infrastructure Encryption, Key Authority, and Secret Protection

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure encryption, key authority, and secret protection for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0005-C07 Oracle Cloud Infrastructure Data Classification, Residency, and Service Selection

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure data classification, residency, and service selection for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0005-C08 Oracle Cloud Infrastructure Workload Identity and Service Authorization

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure workload identity and service authorization for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0005-C09 Oracle Cloud Infrastructure Declarative Provisioning and Change Control

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure declarative provisioning and change control for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0005-C10 Oracle Cloud Infrastructure Artifact, Image, and Software Supply-Chain Assurance

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure artifact, image, and software supply-chain assurance for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0005-C11 Oracle Cloud Infrastructure Logging, Telemetry, and Security Monitoring

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure logging, telemetry, and security monitoring for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0005-C12 Oracle Cloud Infrastructure Reliability, Availability-Zone, and Region Strategy

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure reliability, availability-zone, and region strategy for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0005-C13 Oracle Cloud Infrastructure Backup, Restoration, and Cyber-Recovery

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure backup, restoration, and cyber-recovery for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0005-C14 Oracle Cloud Infrastructure Vulnerability, Configuration, and Drift Management

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure vulnerability, configuration, and drift management for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0005-C15 Oracle Cloud Infrastructure Cost, Quota, Capacity, and FinOps Governance

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure cost, quota, capacity, and finops governance for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0005-C16 Oracle Cloud Infrastructure Incident Response and Provider Escalation

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure incident response and provider escalation for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0005-C17 Oracle Cloud Infrastructure Portability, Exit, and Data Disposition

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure portability, exit, and data disposition for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0005-C18 Oracle Cloud Infrastructure Evidence Package and Periodic Reassessment

The organization MUST define, implement, verify, and maintain oracle cloud infrastructure evidence package and periodic reassessment for in-scope Oracle Cloud Infrastructure architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0005 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0005

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Alibaba Cloud Architecture and Automation Standard

Alibaba Cloud resource hierarchy, RAM identity, network, data residency, automation, resilience, operations, and evidence.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0006

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Alibaba Cloud Architecture and Automation Standard

DOCUMENT ID
MYTHOS-CLD-0006

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy Alibaba Cloud architecture system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

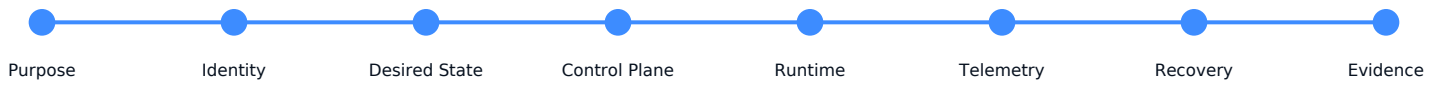
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting Alibaba Cloud architecture capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for Alibaba Cloud architecture across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of Alibaba Cloud architecture capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

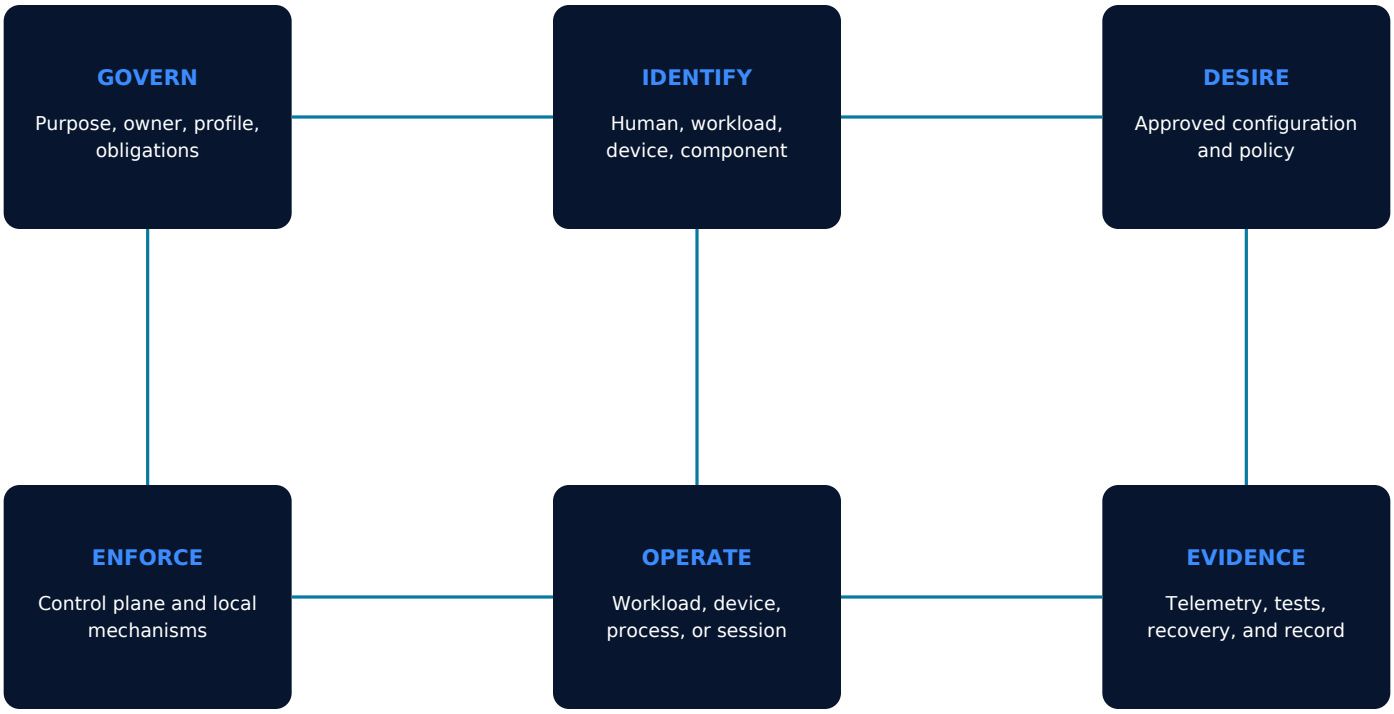
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0006-C01 Alibaba Cloud Tenancy, Organization, and Account Hierarchy

The organization MUST define, implement, verify, and maintain alibaba cloud tenancy, organization, and account hierarchy for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0006-C02 Alibaba Cloud Landing Zone and Environment Segmentation

The organization MUST define, implement, verify, and maintain alibaba cloud landing zone and environment segmentation for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0006-C03 Alibaba Cloud Identity Federation and Privileged Administration

The organization MUST define, implement, verify, and maintain alibaba cloud identity federation and privileged administration for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0006-C04 Alibaba Cloud Resource Policy and Preventive Guardrails

The organization MUST define, implement, verify, and maintain alibaba cloud resource policy and preventive guardrails for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0006-C05 Alibaba Cloud Network Topology, Ingress, and Egress Control

The organization MUST define, implement, verify, and maintain alibaba cloud network topology, ingress, and egress control for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0006-C06 Alibaba Cloud Encryption, Key Authority, and Secret Protection

The organization MUST define, implement, verify, and maintain alibaba cloud encryption, key authority, and secret protection for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0006-C07 Alibaba Cloud Data Classification, Residency, and Service Selection

The organization MUST define, implement, verify, and maintain alibaba cloud data classification, residency, and service selection for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0006-C08 Alibaba Cloud Workload Identity and Service Authorization

The organization MUST define, implement, verify, and maintain alibaba cloud workload identity and service authorization for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0006-C09 Alibaba Cloud Declarative Provisioning and Change Control

The organization MUST define, implement, verify, and maintain alibaba cloud declarative provisioning and change control for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0006-C10 Alibaba Cloud Artifact, Image, and Software Supply-Chain Assurance

The organization MUST define, implement, verify, and maintain alibaba cloud artifact, image, and software supply-chain assurance for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0006-C11 Alibaba Cloud Logging, Telemetry, and Security Monitoring

The organization MUST define, implement, verify, and maintain alibaba cloud logging, telemetry, and security monitoring for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0006-C12 Alibaba Cloud Reliability, Availability-Zone, and Region Strategy

The organization MUST define, implement, verify, and maintain alibaba cloud reliability, availability-zone, and region strategy for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0006-C13 Alibaba Cloud Backup, Restoration, and Cyber-Recovery

The organization MUST define, implement, verify, and maintain alibaba cloud backup, restoration, and cyber-recovery for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0006-C14 Alibaba Cloud Vulnerability, Configuration, and Drift Management

The organization MUST define, implement, verify, and maintain alibaba cloud vulnerability, configuration, and drift management for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0006-C15 Alibaba Cloud Cost, Quota, Capacity, and FinOps Governance

The organization MUST define, implement, verify, and maintain alibaba cloud cost, quota, capacity, and finops governance for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0006-C16 Alibaba Cloud Incident Response and Provider Escalation

The organization MUST define, implement, verify, and maintain alibaba cloud incident response and provider escalation for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0006-C17 Alibaba Cloud Portability, Exit, and Data Disposition

The organization MUST define, implement, verify, and maintain alibaba cloud portability, exit, and data disposition for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0006-C18 Alibaba Cloud Evidence Package and Periodic Reassessment

The organization MUST define, implement, verify, and maintain alibaba cloud evidence package and periodic reassessment for in-scope Alibaba Cloud architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0006 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0006

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Kubernetes, Container Orchestration, and Operator Standard

Cluster governance, API and admission control, workload isolation, image provenance, operators, fleet lifecycle, recovery, and evidence.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0007

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Kubernetes, Container Orchestration, and Operator Standard

DOCUMENT ID
MYTHOS-CLD-0007

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy Kubernetes and container orchestration system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW

Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting Kubernetes and container orchestration capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for Kubernetes and container orchestration across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of Kubernetes and container orchestration capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

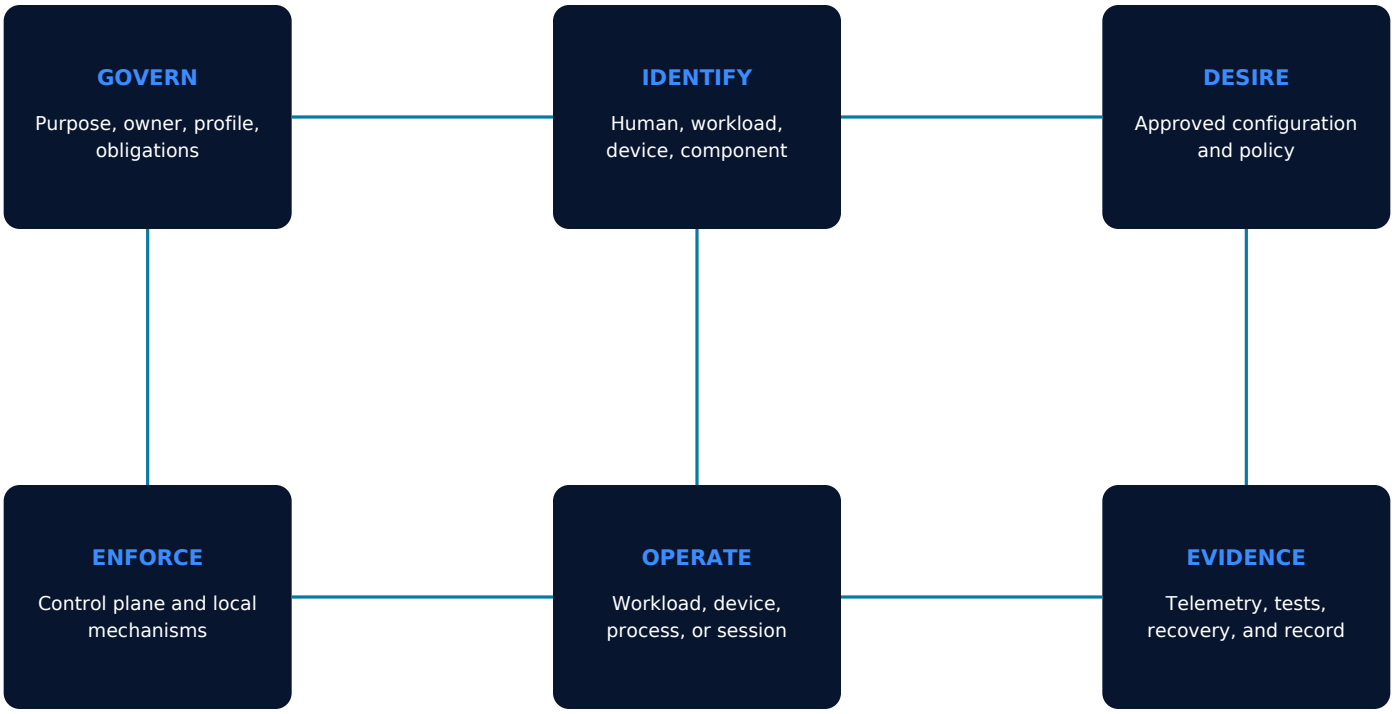
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0007-C01 Cluster Inventory, Ownership, and Criticality

The organization MUST define, implement, verify, and maintain cluster inventory, ownership, and criticality for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0007-C02 API Server Exposure and Administrative Access

The organization MUST define, implement, verify, and maintain api server exposure and administrative access for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0007-C03 Authentication, RBAC, and Service-Account Governance

The organization MUST define, implement, verify, and maintain authentication, rbac, and service-account governance for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0007-C04 Admission Control and Policy Enforcement

The organization MUST define, implement, verify, and maintain admission control and policy enforcement for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0007-C05 Pod Security and Workload Isolation

The organization MUST define, implement, verify, and maintain pod security and workload isolation for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0007-C06 Network Policy, Service Mesh, and Egress Control

The organization MUST define, implement, verify, and maintain network policy, service mesh, and egress control for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0007-C07 Secrets, Certificates, and Key Lifecycle

The organization MUST define, implement, verify, and maintain secrets, certificates, and key lifecycle for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0007-C08 Image Provenance, Signing, and Registry Governance

The organization MUST define, implement, verify, and maintain image provenance, signing, and registry governance for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0007-C09 Node Operating System and Runtime Hardening

The organization MUST define, implement, verify, and maintain node operating system and runtime hardening for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0007-C10 Storage Classes, Persistent Data, and Encryption

The organization MUST define, implement, verify, and maintain storage classes, persistent data, and encryption for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0007-C11 Operator, Controller, and Custom-Resource Governance

The organization MUST define, implement, verify, and maintain operator, controller, and custom-resource governance for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0007-C12 Multi-Tenancy and Namespace Boundary Assurance

The organization MUST define, implement, verify, and maintain multi-tenancy and namespace boundary assurance for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0007-C13 GitOps, Desired State, and Drift Reconciliation

The organization MUST define, implement, verify, and maintain gitops, desired state, and drift reconciliation for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0007-C14 Observability, Audit, and Runtime Detection

The organization MUST define, implement, verify, and maintain observability, audit, and runtime detection for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0007-C15 Backup, Restore, and Cluster Reconstitution

The organization MUST define, implement, verify, and maintain backup, restore, and cluster reconstitution for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0007-C16 Version, Upgrade, and Deprecation Management

The organization MUST define, implement, verify, and maintain version, upgrade, and deprecation management for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0007-C17 Incident Containment and Forensic Preservation

The organization MUST define, implement, verify, and maintain incident containment and forensic preservation for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0007-C18 Fleet Evidence and Periodic Conformance

The organization MUST define, implement, verify, and maintain fleet evidence and periodic conformance for in-scope Kubernetes and container orchestration capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0007 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0007

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Serverless and Event-Driven Compute Standard

Function and event architecture, identity, event contracts, replay, backpressure, observability, recovery, and cost controls.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0008

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Serverless and Event-Driven Compute Standard

DOCUMENT ID
MYTHOS-CLD-0008

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy serverless and event-driven compute system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

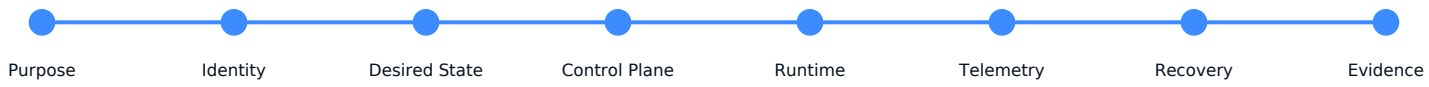
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting serverless and event-driven compute capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for serverless and event-driven compute across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of serverless and event-driven compute capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

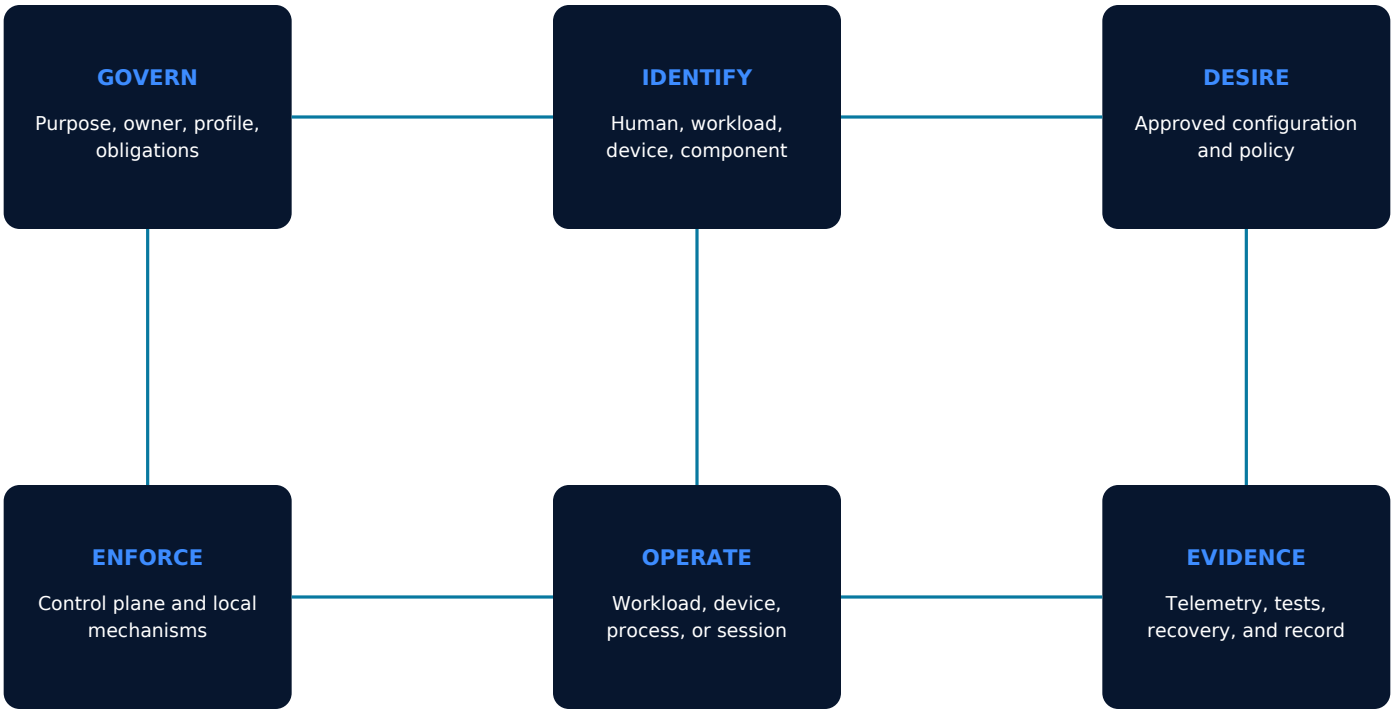
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0008-C01 Function, Service, and Event Inventory

The organization MUST define, implement, verify, and maintain function, service, and event inventory for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0008-C02 Event Contract and Schema Governance

The organization MUST define, implement, verify, and maintain event contract and schema governance for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0008-C03 Trigger Identity and Authorization

The organization MUST define, implement, verify, and maintain trigger identity and authorization for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0008-C04 Workload Identity and Least Privilege

The organization MUST define, implement, verify, and maintain workload identity and least privilege for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0008-C05 Idempotency and Duplicate-Delivery Handling

The organization MUST define, implement, verify, and maintain idempotency and duplicate-delivery handling for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0008-C06 Ordering, Concurrency, and Consistency Semantics

The organization MUST define, implement, verify, and maintain ordering, concurrency, and consistency semantics for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0008-C07 Retry, Timeout, and Dead-Letter Governance

The organization MUST define, implement, verify, and maintain retry, timeout, and dead-letter governance for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0008-C08 Replay, Reprocessing, and Side-Effect Safety

The organization MUST define, implement, verify, and maintain replay, reprocessing, and side-effect safety for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0008-C09 Data Classification and Payload Protection

The organization MUST define, implement, verify, and maintain data classification and payload protection for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0008-C10 Secrets, Configuration, and Environment Isolation

The organization MUST define, implement, verify, and maintain secrets, configuration, and environment isolation for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0008-C11 Network Egress and Service Boundary Control

The organization MUST define, implement, verify, and maintain network egress and service boundary control for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0008-C12 Runtime, Dependency, and Artifact Provenance

The organization MUST define, implement, verify, and maintain runtime, dependency, and artifact provenance for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0008-C13 Scaling, Backpressure, and Saturation Protection

The organization MUST define, implement, verify, and maintain scaling, backpressure, and saturation protection for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0008-C14 Tracing, Correlation, and Operational Evidence

The organization MUST define, implement, verify, and maintain tracing, correlation, and operational evidence for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0008-C15 Cost, Quota, and Invocation-Abuse Controls

The organization MUST define, implement, verify, and maintain cost, quota, and invocation-abuse controls for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0008-C16 Failure Recovery and Regional Continuity

The organization MUST define, implement, verify, and maintain failure recovery and regional continuity for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0008-C17 Representative Testing and Failure Injection

The organization MUST define, implement, verify, and maintain representative testing and failure injection for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0008-C18 Retirement, Event Drainage, and Data Disposition

The organization MUST define, implement, verify, and maintain retirement, event drainage, and data disposition for in-scope serverless and event-driven compute capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0008 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

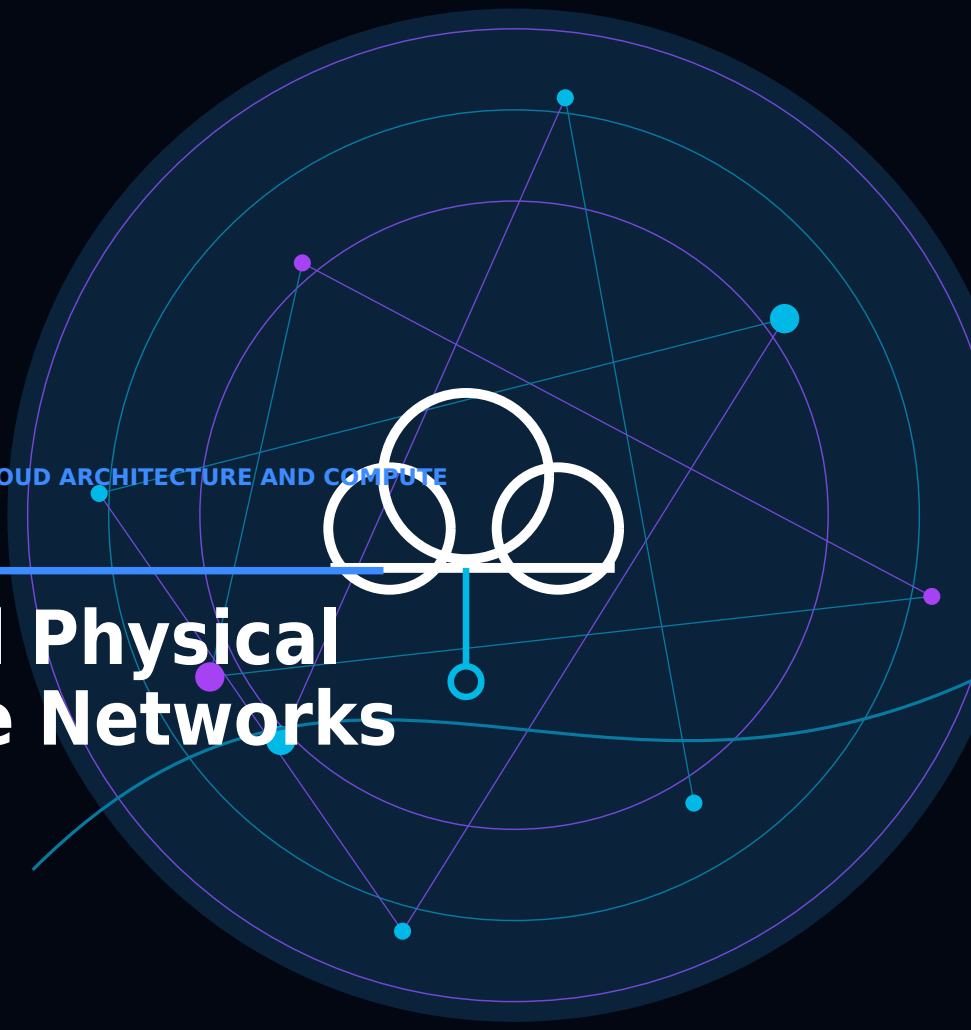
SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0008

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY



ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Decentralized Physical Infrastructure Networks Standard

Distributed-node identity, attestation, measurement, incentives, governance, privacy, resilience, and service evidence.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0009

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Decentralized Physical Infrastructure Networks Standard

DOCUMENT ID
MYTHOS-CLD-0009

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy decentralized physical infrastructure networks system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

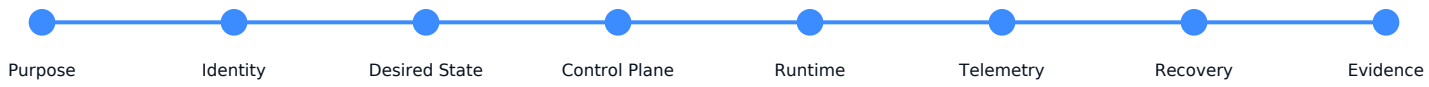
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting decentralized physical infrastructure networks capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for decentralized physical infrastructure networks across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of decentralized physical infrastructure networks capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

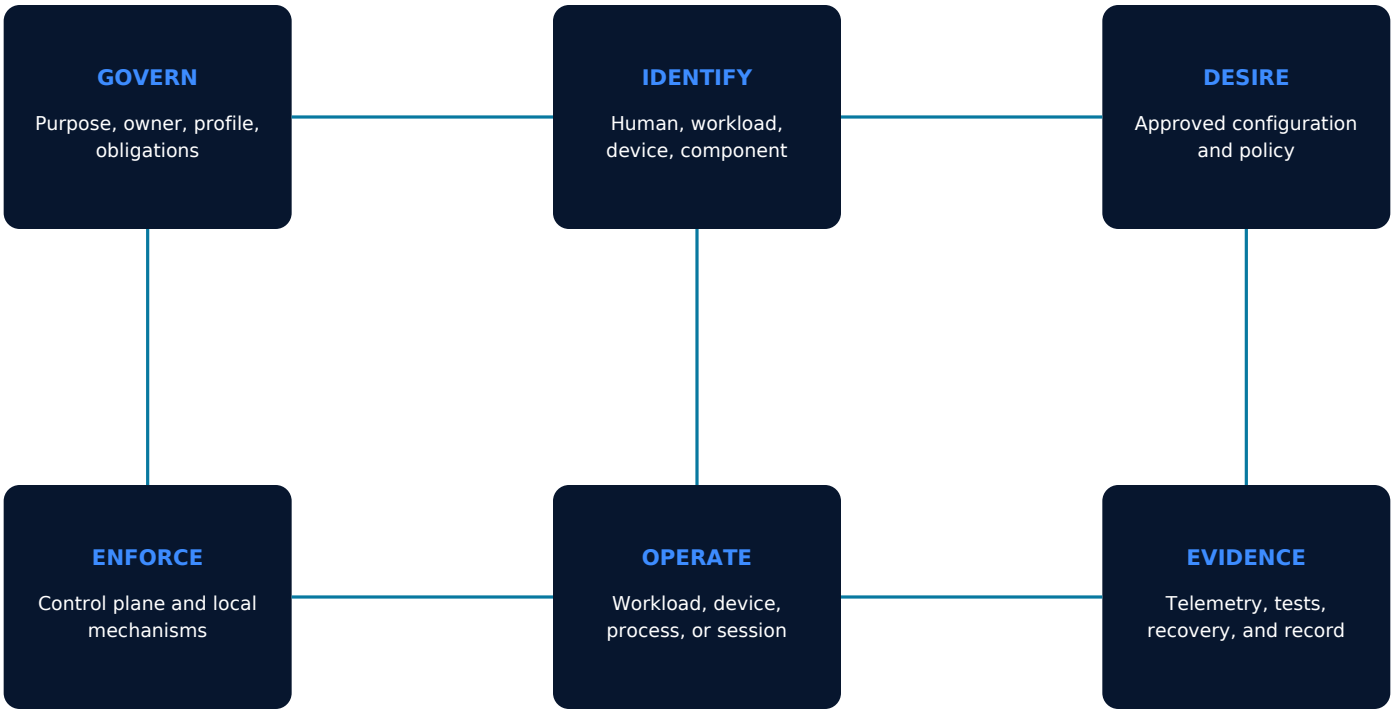
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0009-C01 Service Purpose and Decentralization Rationale

The organization MUST define, implement, verify, and maintain service purpose and decentralization rationale for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0009-C02 Participant, Node, and Operator Identity

The organization MUST define, implement, verify, and maintain participant, node, and operator identity for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0009-C03 Node Enrollment, Attestation, and Revocation

The organization MUST define, implement, verify, and maintain node enrollment, attestation, and revocation for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0009-C04 Sybil Resistance and Duplicate-Resource Detection

The organization MUST define, implement, verify, and maintain sybil resistance and duplicate-resource detection for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0009-C05 Location, Capacity, and Service Measurement

The organization MUST define, implement, verify, and maintain location, capacity, and service measurement for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0009-C06 Proof, Oracle, and Measurement Integrity

The organization MUST define, implement, verify, and maintain proof, oracle, and measurement integrity for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0009-C07 Work Quality and Availability Verification

The organization MUST define, implement, verify, and maintain work quality and availability verification for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0009-C08 Incentive, Reward, and Penalty Design

The organization MUST define, implement, verify, and maintain incentive, reward, and penalty design for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0009-C09 Economic Attack and Collusion Resistance

The organization MUST define, implement, verify, and maintain economic attack and collusion resistance for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0009-C10 Software, Firmware, and Node Configuration

The organization MUST define, implement, verify, and maintain software, firmware, and node configuration for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0009-C11 Data Protection, Privacy, and Jurisdiction

The organization MUST define, implement, verify, and maintain data protection, privacy, and jurisdiction for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0009-C12 Network Exposure and Administrative Access

The organization MUST define, implement, verify, and maintain network exposure and administrative access for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0009-C13 Key Custody and Transaction Authorization

The organization MUST define, implement, verify, and maintain key custody and transaction authorization for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0009-C14 Protocol Governance and Upgrade Authority

The organization MUST define, implement, verify, and maintain protocol governance and upgrade authority for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0009-C15 Dispute, Fraud, and Appeals Process

The organization MUST define, implement, verify, and maintain dispute, fraud, and appeals process for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0009-C16 Availability, Partition, and Recovery Behavior

The organization MUST define, implement, verify, and maintain availability, partition, and recovery behavior for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0009-C17 Legal, Tax, Sanctions, and Supplier Boundaries

The organization MUST define, implement, verify, and maintain legal, tax, sanctions, and supplier boundaries for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0009-C18 Exit, Migration, and Evidence Preservation

The organization MUST define, implement, verify, and maintain exit, migration, and evidence preservation for in-scope decentralized physical infrastructure networks capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0009 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0009

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Private Cloud, Hypervisor, and Bare-Metal Standard

Private-cloud and virtualization governance, management-plane security, tenant isolation, hardware lifecycle, capacity, recovery, and evidence.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0010

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Private Cloud, Hypervisor, and Bare-Metal Standard

DOCUMENT ID
MYTHOS-CLD-0010

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy private cloud, hypervisor, and bare metal system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW

Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting private cloud, hypervisor, and bare metal capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for private cloud, hypervisor, and bare metal across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of private cloud, hypervisor, and bare metal capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

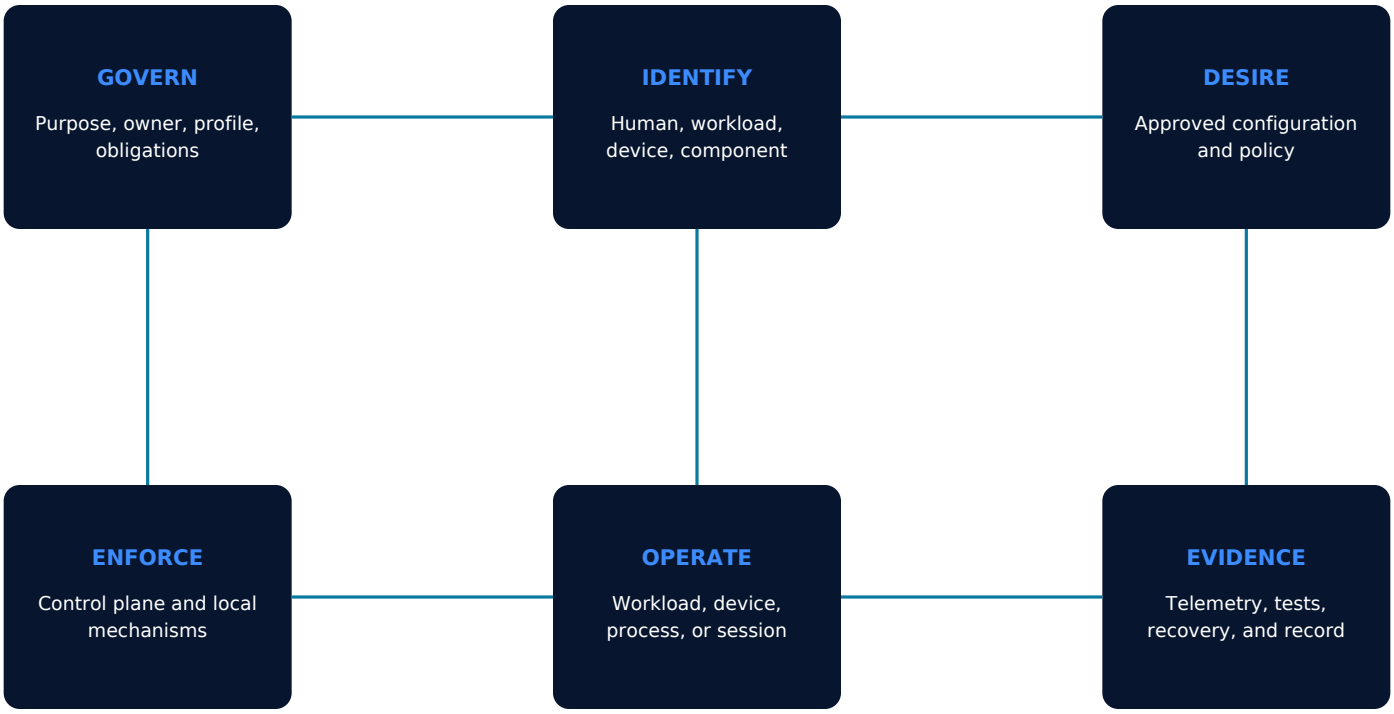
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0010-C01 Private Cloud Service Boundary and Ownership

The organization MUST define, implement, verify, and maintain private cloud service boundary and ownership for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0010-C02 Facility, Power, Cooling, and Physical Dependency

The organization MUST define, implement, verify, and maintain facility, power, cooling, and physical dependency for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0010-C03 Hardware Inventory and Lifecycle Governance

The organization MUST define, implement, verify, and maintain hardware inventory and lifecycle governance for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0010-C04 BMC, Out-of-Band, and Management Network Isolation

The organization MUST define, implement, verify, and maintain bmc, out-of-band, and management network isolation for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0010-C05 Hypervisor and Management-Plane Hardening

The organization MUST define, implement, verify, and maintain hypervisor and management-plane hardening for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0010-C06 Administrative Identity and Privileged Access

The organization MUST define, implement, verify, and maintain administrative identity and privileged access for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0010-C07 Tenant, Project, and Resource Isolation

The organization MUST define, implement, verify, and maintain tenant, project, and resource isolation for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0010-C08 Virtual Network and Storage Segmentation

The organization MUST define, implement, verify, and maintain virtual network and storage segmentation for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0010-C09 Golden Images, Templates, and Artifact Provenance

The organization MUST define, implement, verify, and maintain golden images, templates, and artifact provenance for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0010-C10 Bare-Metal Provisioning and Sanitization

The organization MUST define, implement, verify, and maintain bare-metal provisioning and sanitization for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0010-C11 Patch, Firmware, and Compatibility Management

The organization MUST define, implement, verify, and maintain patch, firmware, and compatibility management for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0010-C12 Capacity, Overcommit, and Performance Governance

The organization MUST define, implement, verify, and maintain capacity, overcommit, and performance governance for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0010-C13 Telemetry, Configuration, and Drift Detection

The organization MUST define, implement, verify, and maintain telemetry, configuration, and drift detection for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0010-C14 Backup, Snapshot, and Restoration Assurance

The organization MUST define, implement, verify, and maintain backup, snapshot, and restoration assurance for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0010-C15 Cluster Failure and Management-Plane Recovery

The organization MUST define, implement, verify, and maintain cluster failure and management-plane recovery for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0010-C16 Incident Containment and Forensic Readiness

The organization MUST define, implement, verify, and maintain incident containment and forensic readiness for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0010-C17 Supplier Support, Spares, and End-of-Life Planning

The organization MUST define, implement, verify, and maintain supplier support, spares, and end-of-life planning for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0010-C18 Reconstitution, Exit, and Evidence Package

The organization MUST define, implement, verify, and maintain reconstitution, exit, and evidence package for in-scope private cloud, hypervisor, and bare metal capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

MINIMUM DEPTH

Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0010 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

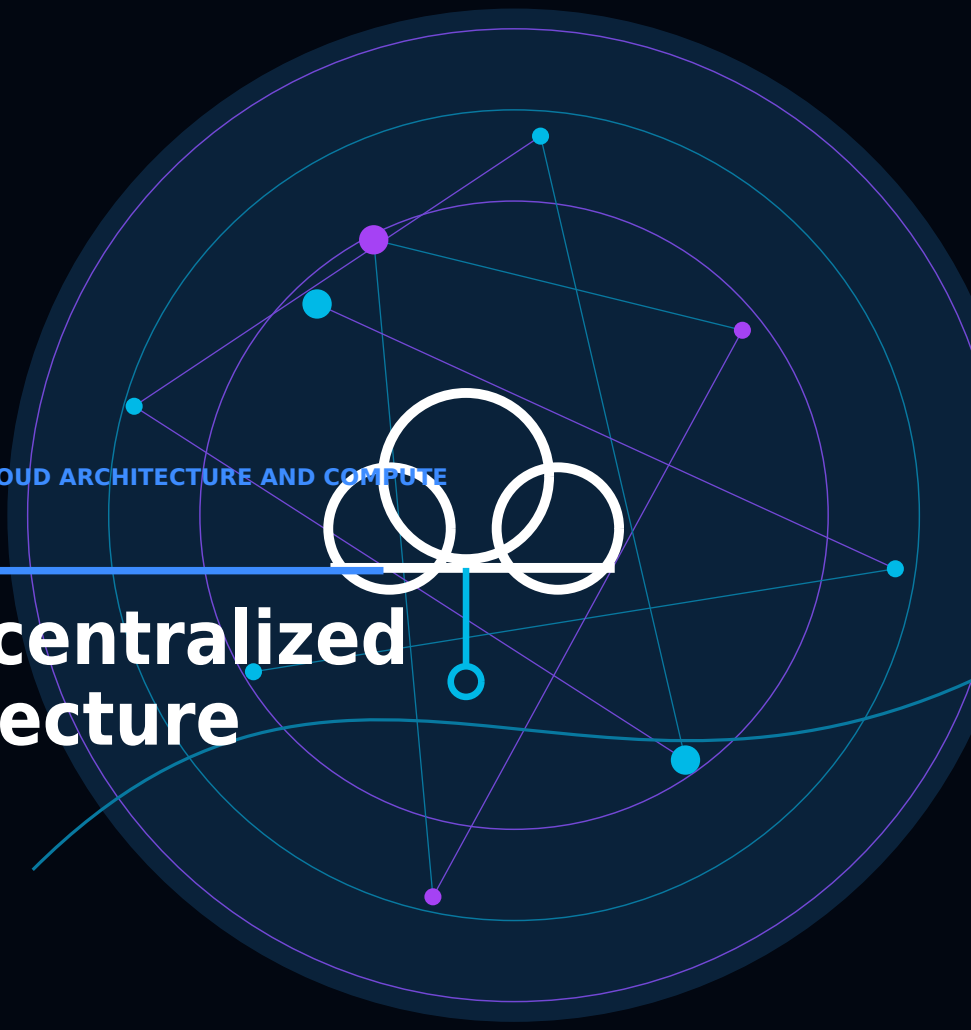
SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0010

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY



ENGINEERING STANDARDS LIBRARY / CLOUD ARCHITECTURE AND COMPUTE

Web3 and Decentralized Ledger Architecture Standard

Distributed-ledger architecture, smart contracts, custody, oracle, bridge, governance, monitoring, recovery, and retirement.

PERMANENT DOCUMENT ID

MYTHOS-CLD-0011

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Web3 and Decentralized Ledger Architecture Standard

DOCUMENT ID
MYTHOS-CLD-0011

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Cloud Architecture and Compute

A trustworthy Web3 and decentralized ledger architecture system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

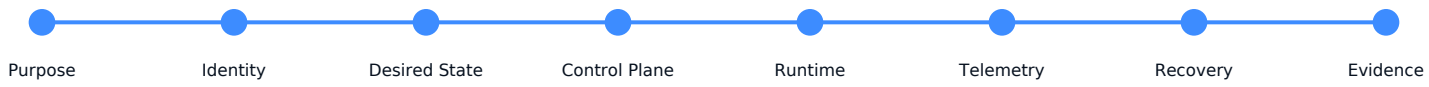
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting Web3 and decentralized ledger architecture capabilities MUST define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for Web3 and decentralized ledger architecture across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of Web3 and decentralized ledger architecture capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

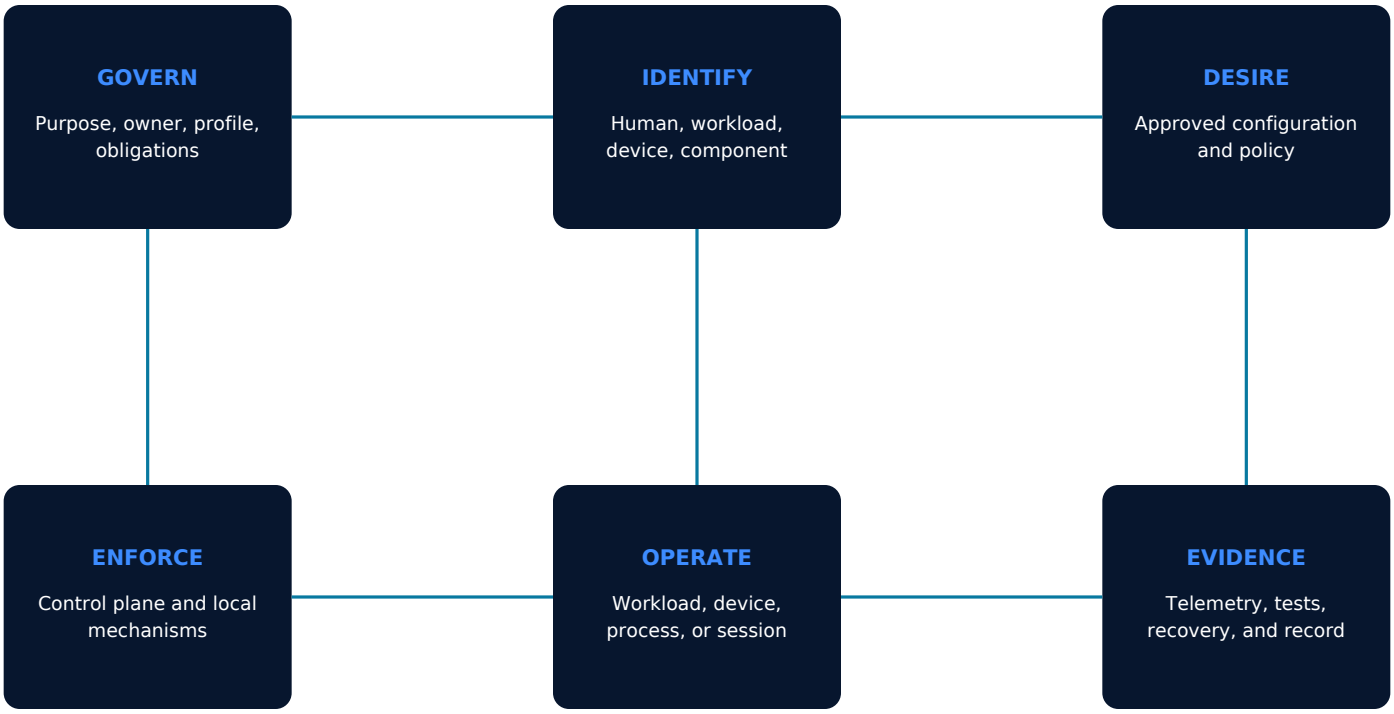
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes MUST be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy MUST be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state MUST be compared with approved desired state and material drift MUST trigger response.
- Safety and continuity mechanisms MUST remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence MUST be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-CLD-0011-C01 Use-Case Justification and Trust Assumptions

The organization MUST define, implement, verify, and maintain use-case justification and trust assumptions for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0011-C02 Network, Consensus, and Finality Selection

The organization MUST define, implement, verify, and maintain network, consensus, and finality selection for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0011-C03 Node, Validator, and Client Governance

The organization MUST define, implement, verify, and maintain node, validator, and client governance for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0011-C04 Key Custody, Wallet, and Transaction Authorization

The organization MUST define, implement, verify, and maintain key custody, wallet, and transaction authorization for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-CLD-0011-C05 Smart-Contract Design and Upgrade Authority

The organization MUST define, implement, verify, and maintain smart-contract design and upgrade authority for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0011-C06 Secure Development, Review, and Formal Analysis

The organization MUST define, implement, verify, and maintain secure development, review, and formal analysis for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0011-C07 Oracle, Data Feed, and External-State Integrity

The organization MUST define, implement, verify, and maintain oracle, data feed, and external-state integrity for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0011-C08 Bridge, Interoperability, and Cross-Chain Risk

The organization MUST define, implement, verify, and maintain bridge, interoperability, and cross-chain risk for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-CLD-0011-C09 Token, Incentive, and Economic-Security Design

The organization MUST define, implement, verify, and maintain token, incentive, and economic-security design for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0011-C10 Privacy, Confidentiality, and Metadata Exposure

The organization MUST define, implement, verify, and maintain privacy, confidentiality, and metadata exposure for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0011-C11 Identity, Compliance, and Jurisdictional Boundaries

The organization MUST define, implement, verify, and maintain identity, compliance, and jurisdictional boundaries for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-CLD-0011-C12 Transaction Monitoring and Abuse Detection

The organization MUST define, implement, verify, and maintain transaction monitoring and abuse detection for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-CLD-0011-C13 Availability, Congestion, and Fee Volatility

The organization MUST define, implement, verify, and maintain availability, congestion, and fee volatility for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-CLD-0011-C14 Fork, Reorganization, and Governance Response

The organization MUST define, implement, verify, and maintain fork, reorganization, and governance response for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-CLD-0011-C15 Incident Pause, Recovery, and Asset Protection

The organization MUST define, implement, verify, and maintain incident pause, recovery, and asset protection for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-CLD-0011-C16 Dependency, Library, and Client Supply Chain

The organization MUST define, implement, verify, and maintain dependency, library, and client supply chain for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-CLD-0011-C17 Migration, Contract Retirement, and Key Destruction

The organization MUST define, implement, verify, and maintain migration, contract retirement, and key destruction for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-CLD-0011-C18 Evidence, Disclosure, and Periodic Reassessment

The organization MUST define, implement, verify, and maintain evidence, disclosure, and periodic reassessment for in-scope Web3 and decentralized ledger architecture capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds MUST be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

CONTROL-PLANE COMPROMISE

An administrative or orchestration plane can alter broad production scope.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER OR REGION DEPENDENCY

A provider, region, identity, DNS, or service dependency fails without a tested alternative.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CONFIGURATION DRIFT

Runtime state diverges from approved desired state without timely detection.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SOVEREIGNTY BREACH

Data or keys move through an unapproved jurisdiction or subprocess.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

COST AND QUOTA RUNAWAY

Unbounded scaling, abuse, or configuration error exhausts budget or service limits.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EXIT FAILURE

Workloads, data, identity, or evidence cannot be migrated within the required time.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

	FOUNDATIONAL	ADVANCED	HIGH ASSURANCE
TYPICAL SCOPE	Low consequence, limited autonomy, non-sensitive data, reversible outputs.	Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.	Safety, security, regulated, financial, identity, or broadly consequential use.
MINIMUM DEPTH	Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.	Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.	Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1. **CONCEPT**
   Purpose, owner, impact, boundaries
2. **DESIGN**
   Architecture, threat, data, identity
3. **BUILD**
   Controlled implementation and provenance
4. **EVALUATE**
   Representative, adversarial, recovery tests
5. **RELEASE**
   Approval, canary, rollback, evidence
6. **OPERATE**
   Observe, support, detect, respond
7. **CHANGE**
   Reassess, compare, gate, reverse
8. **RETIRE**
   Revoke, export, dispose, preserve

LIFECYCLE INVARIANT

Every stage MUST leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS

Establish ownership and truth

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS

Create enforceable boundaries

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS

Prove recovery and operating control

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS

Scale assurance

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE

Named, versioned capability and deployment boundary.

PROFILE

Foundational, Advanced, or High Assurance with trigger rationale.

SCOPE

Workloads, users, data, tools, regions, providers, and exclusions.

CRITERIA

Pass, partial, fail, not applicable, and exception status for every criterion.

EVIDENCE

Artifact references, evidence grade, date, environment, and reproducibility.

LIMITATIONS

Known failure modes, unsupported workloads, uncertainty, and residual risk.

EXCEPTIONS

Owner, rationale, compensating control, expiration, and approval.

VALIDITY

Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0	**Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5	**Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

CSA CCM v4	**Cloud Controls Matrix**

https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud control domains and shared-responsibility assessment structure.

FinOps Framework	**FinOps Framework**

https://www.finops.org/framework/

Cloud value, cost, usage, ownership, and operating-practice guidance.

NIST SP 800-204A	**Building Secure Microservices-based Applications Using Service-Mesh Architecture**

https://doi.org/10.6028/NIST.SP.800-204A

Microservice and service-mesh security architecture.

CNCF Cloud Native Security	**Cloud Native Security Whitepaper**

https://github.com/cncf/tag-security/tree/main/security-whitepaper

Cloud-native lifecycle, supply-chain, runtime, and operations guidance.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-CLD-0011 / CLOUD ARCHITECTURE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

PERMANENT IDENTITY The document ID remains stable across revisions; batch or production sequence metadata is not public identity.

CHANGE CONTROL Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.

SUPERSESSION A superseded edition remains traceable; current routes and catalogs identify the active edition.

CORRECTION Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.

ARCHIVAL INTEGRITY Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-CLD-0011

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY