MYTHOS SYSTEMS

PERMANENT LIBRARY PUBLICATION

ENGINEERING STANDARDS LIBRARY / NETWORK ENGINEERING

Physical Layer, Cabling, Optics, and Data-Center Topology Standard

Defines cabling, optics, facilities interfaces, topology, labeling, testing, and lifecycle.

PERMANENT DOCUMENT ID
MYTHOS-NET-0009

PUBLICATION
Candidate Standard

ASSURANCE SURFACE
6 Atomic Criteria / 6 Families

PERMANENT PUBLICATION IDENTITY

Physical Layer, Cabling, Optics, and Data-Center Topology Standard

Defines cabling, optics, facilities interfaces, topology, labeling, testing, and lifecycle.

DOCUMENT ID
MYTHOS-NET-0009

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-23

SCHEDULED REVIEW
2027-01-23

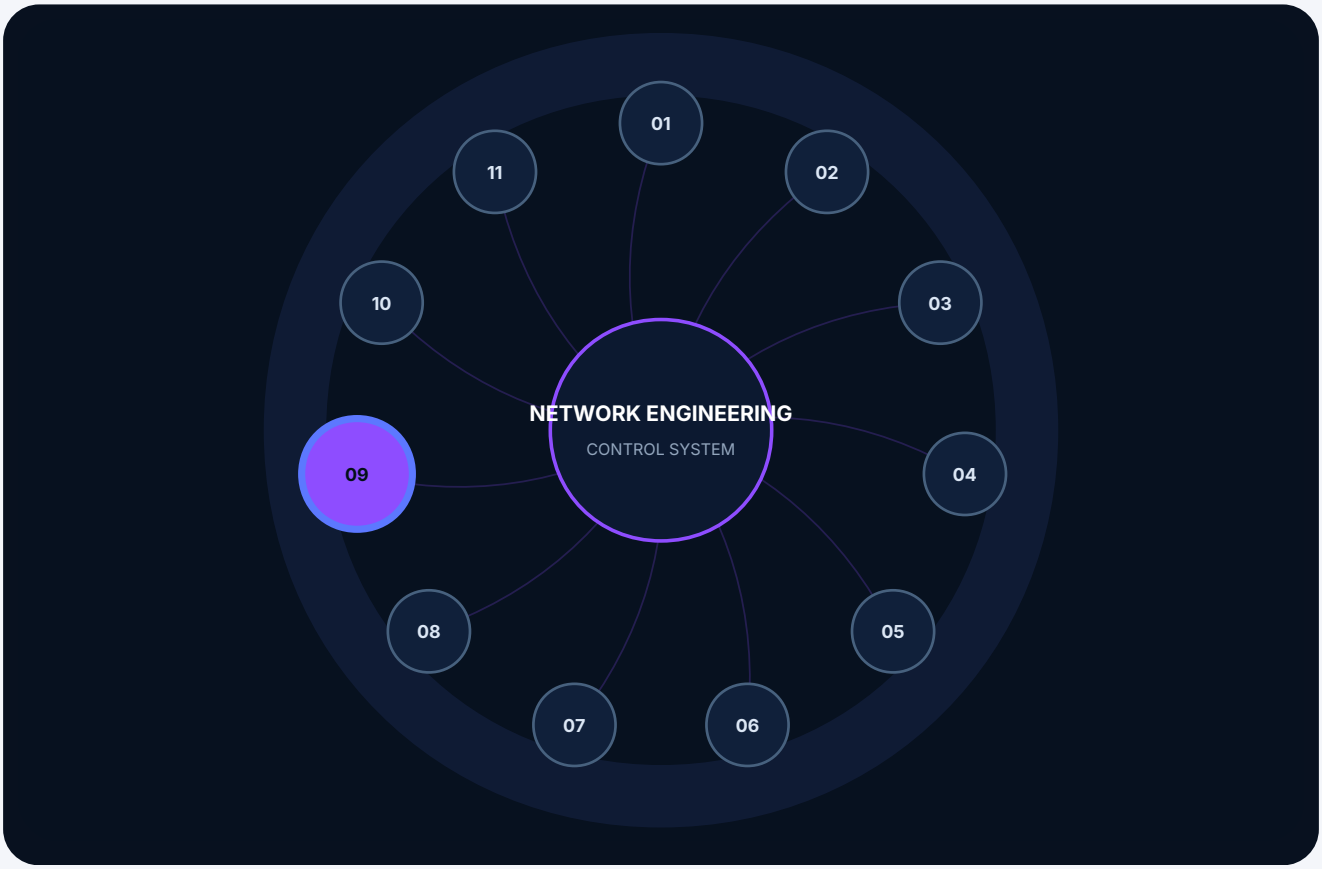
CLASSIFICATION
Public

6	6	4	1
ATOMIC CRITERIA	CAPABILITY FAMILIES	ASSESSMENT PROFILES	PERMANENT IDENTITY

Publication doctrine. This standard establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, recorded evidence, and formal revision history.

DOMAIN CONTROL SYSTEM

MYTHOS-NET-0009 inside the network engineering standard constellation



Connected assurance

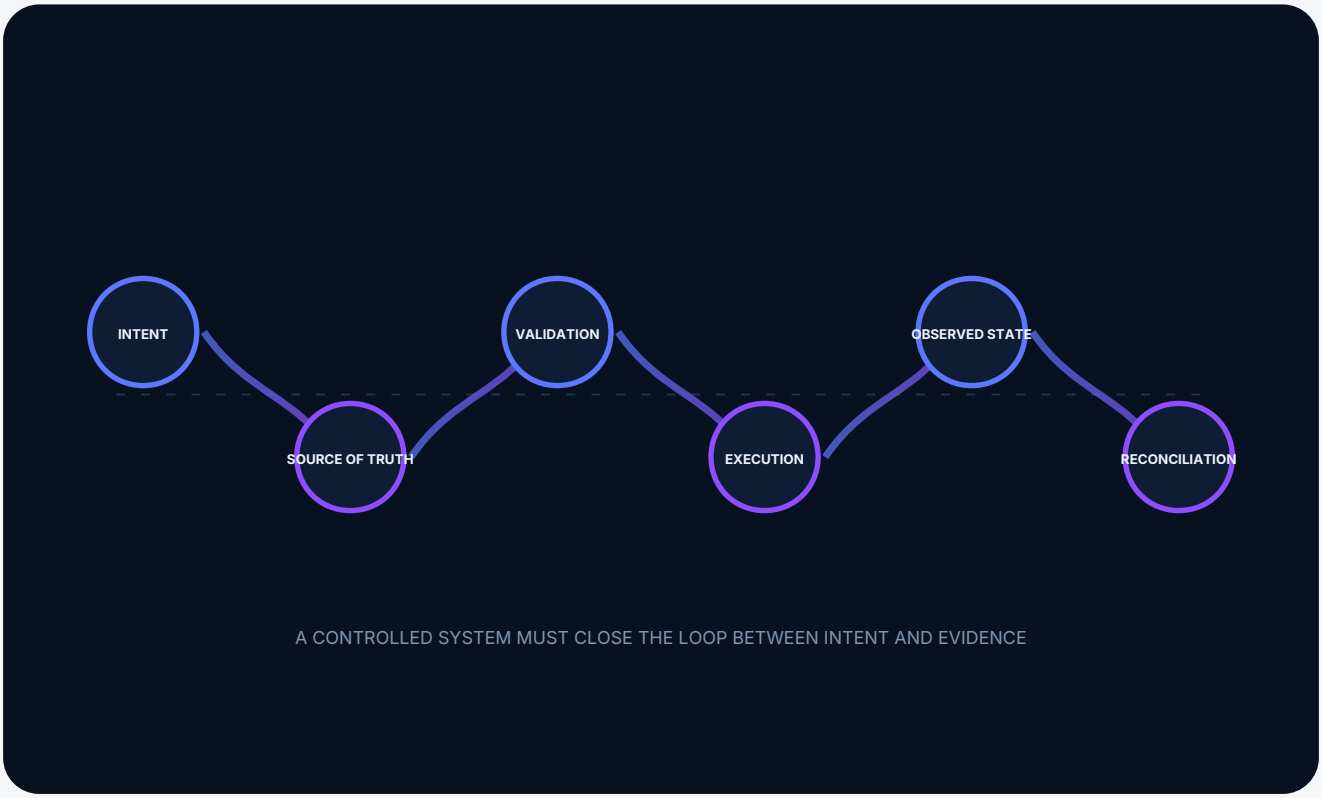
Architecture, policy, implementation, operations, and evidence are evaluated as one controlled system.

Specialization rule

Companion standards may add precision, but they cannot silently weaken this publication's requirements.

CLOSED-LOOP ARCHITECTURE

Intent becomes trustworthy only when observed state returns as evidence



State separation

Desired, approved, deployed, observed, historical, and simulated states must remain distinguishable.

Recoverable change

Material change requires validation, authorization, monitoring, containment, and a credible recovery path.

EVALUATION TOPOLOGY

The capability families and atomic criteria of MYTHOS-NET-0009

Capability families

Families expose the major engineering surfaces and preserve the source weighting model.

Atomic criteria

Each criterion carries a question, maturity spectrum, evidence expectations, assessment method, and operational signals.

NAVIGATION

Contents

ENGINEERING DOCTRINE

0. Executive Mandate

The architecture of the physical datacenter has failed.

Organizations spend millions on high-availability cloud architectures and distributed state machines, only to house them in datacenters where a single misrouted cable takes down a core switch, a blocked CRAC unit causes thermal throttling, and unlabeled fiber strands result in hours of downtime. Physical infrastructure is treated as mere "plumbing" rather than the foundational Layer 1 upon which all zero-trust and AI compute paradigms rely.

This standard exists because:

1. **Spaghetti Cabling is a Security and Operational Threat:** An unorganized, unlabeled cable plant guarantees extended outages. When a patch cable fails, engineers must trace it through a rat's nest of wires, increasing Mean Time to Recovery (MTTR) from seconds to hours. Structured cabling with strict color-coding and mandatory labeling is a prerequisite for production.
2. **Thermals Dictate Compute Density:** Modern AI GPU clusters (e.g., NVIDIA Hopper/Blackwell) draw 10kW+ per rack. Traditional datacenter cooling (perforated tiles, hot/cold aisle) is insufficient. Organizations MUST implement containment strategies, in-row cooling, or direct-to-chip liquid cooling to prevent thermal throttling and hardware degradation.
3. **Single-Point Power is high-risk architectural constraint:** A server plugged into a single PDU, or a rack fed by a single power feed, is a ticking time bomb. Production systems MUST have A/B power diversity, from the UPS down to the server's redundant power supplies, capable of surviving a single-phase or single-feed failure.
4. **The Physical Layer Must Be Software-Defined:** Treating the datacenter as a static physical entity is obsolete. Organizations MUST utilize DCIM (Datacenter Infrastructure Management) tools to monitor power draw, temperature, and humidity in real-time, treating power and cooling as consumable, programmable resources.

This document establishes the **Mythos Physical Infrastructure Standard (MPIS)**, a comprehensive, evidence-based methodology for evaluating datacenter topologies, cabling rigor, and environmental resilience.

ENGINEERING DOCTRINE

Part I. Scope and Applicability

1.1 In Scope

This standard covers the evaluation of:

- Structured cabling (Copper Cat6a/Cat8, Fiber OM4/OM5/OS2)
- Cable color-coding, labeling (TIA-606-C), and management (hook-and-loop vs. zip ties)
- Datacenter topology (Hot/Cold aisle containment, rack layouts)
- Power distribution (A/B feeds, PDUs, UPS, generators)
- Cooling and thermal management (In-row, liquid cooling, blanking panels)
- Environmental monitoring (DCIM, leak detection, temperature/humidity sensors)

1.2 Out of Scope

- Logical network topology and routing protocols (covered in MYTHOS-NET-0001)
- Hardware specifications (covered in MYTHOS-HW-0001)
- General disaster recovery (covered in MYTHOS-SRE-0002)

1.3 Audience

- Datacenter facility managers and mechanical engineers
- Network engineers and cable plant technicians
- IT operations and infrastructure architects
- Hardware procurement teams
- Standards bodies seeking a reference physical infrastructure methodology

---

ENGINEERING DOCTRINE

Part II. Definitions and Taxonomy

2.1 Physical Dimensions

Dimension	Definition
Structured Cabling	A standardized architecture for telecommunications cabling, using dedicated pathways, patch panels, and strict labeling to ensure modularity and ease of management.
A/B Power Diversity	An architectural paradigm where critical infrastructure receives power from two completely independent electrical feeds (UPS A and UPS B), terminating on dual power supplies in the server.
Hot/Cold Aisle Containment	A datacenter cooling strategy where server racks are arranged in alternating rows (hot and cold), and physical barriers are used to prevent hot exhaust air from mixing with cold intake air.
DCIM	Datacenter Infrastructure Management. Software tools that monitor, measure, and manage datacenter resources (power, cooling, space, connectivity) in real-time.
OM5 Fiber	Wideband multimode fiber optimized for Short Wavelength Division Multiplexing (SWDM), allowing multiple wavelengths over a single fiber pair for high-density datacenter backbones.

2.2 The Physical Infrastructure Doctrine

> An unlabeled cable is a liability. A single power feed is a single point of failure. Mixed airflow is a thermal bottleneck. If the physical layer is not structured, the logical layer is an illusion.

ENGINEERING DOCTRINE

Part III. Evaluation Methodology

3.1 Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; spaghetti cabling, single power feed, no containment, thermal hotspots
1	Basic labeling exists, but inconsistent power and cooling
2	Functional A/B power, but lacks strict color-coding or DCIM monitoring
3	Solid production performance; strict TIA-606-C labeling, A/B power, hot/cold containment, DCIM
4	Strong performance; liquid cooling for high-density, automated environmental alerts
5	Best-in-class; sets the standard for mathematically verified, autonomous physical resilience

Weighting

Category	Weight	Rationale
Cabling Structure & Labeling	20%	Untraceable cables cause massive MTTR during outages
Power Redundancy & Diversity	20%	A single power event should never take down a production node
Cooling & Airflow Containment	20%	High-density AI compute requires strict thermal management
Environmental Monitoring (DCIM)	15%	Blindness to power/thermal data leads to cascading failures
Physical Security & Access	15%	Unlocked racks allow physical tampering and cable tapping
Rack Density & Space Utilization	10%	Poor space planning halts scaling capabilities

Total: 100%

A system MUST score at least 3.0 in Cabling Structure and Power Redundancy to be considered for production use.

EVALUATION AND ASSURANCE SYSTEM

Capability claims are bounded by evidence, context, and reproducible assessment.

6 atomic criteria across 6 capability families define the evaluation surface of this standard.

4.1 / CAPABILITY FAMILY

Cabling Structure and Labeling

SOURCE WEIGHT 20%

4.1.1
Structured Plant Rigor

MYTHOS-NET-0009-EVAL-4.1.1

Structured Plant Rigor

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Cabling Structure and Labeling	**4.1.1**	**20%**	**Evidence-led**

Is the cabling plant strictly organized, color-coded, and traceable?

0
Tangled "spaghetti" cabling; zip ties used; no labels

1
Basic patch panels used, but inconsistent labeling and color coding

2
TIA-606-C compliant labels at both ends; hook-and-loop straps used

3
Strict color-coding enforced (e.g., Red = Security, Blue = Copper, Orange = Internal Fiber, Yellow = Out-of-Band)

4
Cable paths documented in DCIM; fiber optic OTDR (Optical Time-Domain Reflectometer) traces mapped

5
Leading structure: formally verified cable topologies, zero undocumented strands, automated patch-port validation

ENGINEERING INTERPRETATION

This criterion evaluates whether structured plant rigor is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.2 / CAPABILITY FAMILY

Power Redundancy and Diversity

SOURCE WEIGHT 20%

4.2.1
Electrical Resilience

MYTHOS-NET-0009-EVAL-4.2.1

Electrical Resilience

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Power Redundancy and Diversity	**4.2.1**	**20%**	**Evidence-led**

Can a server survive the loss of a single power feed or UPS?

0
Single PDU per rack; single power supply in servers

1
Dual PDUs, but fed from the same UPS

2
A/B power feeds from diverse UPS systems; servers have dual PSUs

3
A/B feeds from diverse generator/ transformer sources; automated transfer switches (ATS) tested regularly

4
Rack-level power monitoring (per outlet) with automated capping to prevent breaker trips

5
Leading resilience: formally verified power diversity, zero single points of failure from grid to server, sub-second failover

ENGINEERING INTERPRETATION

This criterion evaluates whether electrical resilience is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.3 / CAPABILITY FAMILY

Cooling and Airflow Containment

SOURCE WEIGHT 20%

4.3.1
Thermal Management

MYTHOS-NET-0009-EVAL-4.3.1

Thermal Management

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Cooling and Airflow Containment	4.3.1	20%	Evidence-led

Is the datacenter capable of cooling high-density AI racks without throttling?

0
Mixed airflow (some racks face front, some back); no blanking panels

1
Basic hot/cold aisle alignment, but no containment

2
Physical containment (doors/end-of-row panels) separating hot and cold aisles

3
In-row cooling deployed for high-density AI/GPU racks (>15kW)

4
Direct-to-chip liquid cooling (DLC) for extreme-density clusters (>40kW)

5
Leading cooling: formally verified Computational Fluid Dynamics (CFD), zero thermal hotspots, dynamic fan/pump scaling based on real-time CPU/GPU thermals

ENGINEERING INTERPRETATION

This criterion evaluates whether thermal management is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.4 / CAPABILITY FAMILY

Environmental Monitoring (DCIM)

SOURCE WEIGHT 15%

4.4.1
Facility Observability

MYTHOS-NET-0009-EVAL-4.4.1

Facility Observability

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Environmental Monitoring (DCIM)	4.4.1	15%	Evidence-led

Is the physical environment monitored with the same rigor as the application stack?

0
No environmental monitoring; relies on server internal sensors

1
Basic temperature sensors in the room

2
Per-rack temperature and humidity sensors

3
Comprehensive DCIM platform tracking power, cooling, and space; leak detection under raised floors

4
Integration of DCIM with ITSM (e.g., auto-generating tickets when a UPS battery fails)

5
Leading observability: formally verified sensor grids, AI-driven predictive cooling, zero blind spots in facility telemetry

ENGINEERING INTERPRETATION

This criterion evaluates whether facility observability is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.5 / CAPABILITY FAMILY

Physical Security and Access

SOURCE WEIGHT 15%

4.5.1
Access Control

MYTHOS-NET-0009-EVAL-4.5.1

Access Control

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Physical Security and Access	**4.5.1**	**15%**	**Evidence-led**

How is physical access to the datacenter and individual racks governed?

0
Unlocked server room; open racks

1
Single badge reader on the datacenter door

2
Biometric (fingerprint/retina) access on datacenter entry; locked cabinets

3
Mantrap (interlocking doors) at datacenter entry; CCTV covering all aisles

4
Per-rack electronic locks tied to centralized identity (e.g., audited access logs per cabinet)

5
Leading security: formally verified zero-trust physical access, cryptographic attestation of rack entry, zero tailgating potential

ENGINEERING INTERPRETATION

This criterion evaluates whether access control is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.6 / CAPABILITY FAMILY

Rack Density and Space Utilization

SOURCE WEIGHT 10%

4.6.1
Scalability

MYTHOS-NET-0009-EVAL-4.6.1

Scalability

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Rack Density and Space Utilization	**4.6.1**	**10%**	**Evidence-led**

Is the physical space utilized efficiently to allow for future scaling?

0
Ad-hoc rack layouts; wasted space; no weight limits considered

1
Basic rack standards, but no power/ cooling capacity planning

2
Standardized rack elevations documented in DCIM

3
Power and cooling capacity mapped to physical space; new deployments validated against constraints

4
High-density zones established for GPU clusters; standard zones for storage/ network

5
Leading utilization: formally verified space/power/cooling algorithms, zero stranded capacity, optimal workload placement

ENGINEERING INTERPRETATION

This criterion evaluates whether scalability is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

LIFECYCLE AND ASSURANCE

Part V. The Mythos Physical Infrastructure Suite (MPIS)

Traditional facility audits measure uptime. The MPIS evaluates cable traceability, power failover, and thermal resilience under load.

5.1 Suite Composition

5.1.1 MPIS-Cable

- **Blind Trace Test:** 100+ tests requiring a technician to trace a specific port to its origin without visual inspection, verifying the DCIM and labeling system allows instant identification.
- **OTDR Validation:** 50+ tests running Optical Time-Domain Reflectometer scans to verify fiber pairs match documented paths and have no micro-bends.

5.1.2 MPIS-PowerThermal

- **Feed Failure Simulation:** 50+ tests simulating the loss of Power Feed A, verifying all servers seamlessly failover to Feed B without dropping packets.
- **Thermal Soak Test:** 50+ tests running GPU clusters at 100% utilization for 4 hours, verifying containment and cooling systems prevent thermal throttling.

5.2 Execution Protocol

PUBLICATION BOUNDARY

Candidate standard. Permanent identity. Evidence before authority.

Approval requires designated technical, security, legal, accessibility, and governance review with recorded findings and dispositions.